Formalización de una estrategia de protección de microrredes dentro de una arquitectura de red

Juan David Orozco Álvarez

Formalización de una estrategia de protección de microrredes dentro de una arquitectura de red

Juan David Orozco Álvarez

Trabajo de grado presentado como requisito
parcial para optar al tt́ulo de
Ingeniero Electricista

Pereira, Julio de 2019
UNIVERSIDAD TECNOLÓGICA DE PEREIRA
Programa de Ingeniería Eléctrica.

Formalización de una estrategia de protección de microrredes dentro de una arquitectura de red

Director: Juan José Mora Flórez
Codirector: Andrés Ricardo Herrera Orozco

Pereira, Julio de 2019
Programa de Ingeniería Eléctrica.
Universidad Tecnológica de Pereira
La Julita. Pereira(Colombia)
TEL: (+57)(6)3137122
www.utp.edu.co
Versión web disponible en: *http://recursosbiblioteca.utp.edu.co/tesisd/index.html*

Agradecimientos

A mi madre Marina, a quien se le dificultó en estos cinco años, recordar el programa que elegí, sin embargo, siempre me entrega su amor incondicional; y a mi padre Juan de Dios, que nos mantiene alegres sin importar las circunstancias. A ellos, los pilares de mi vida y a quienes más amo, infinitas gracias.

A mis hermanos Esteban y Alexander por el apoyo y a quienes les deseo lo mejor en su vida.

A mis compañeros Camilo, Valentina, Daniela, Carlos y Alejandro por coincidir, por la unión y por las experiencias compartidas.

Y a mis maestros y amigos Juan José y Andrés Ricardo por compartir su sabiduría y ofrecer su acompañamiento durante todo este proceso.

Tabla de Contenido

Capítulo 1

Introducción

En este capítulo se define el problema que motiva la investigación, relacionado con la formalización de estrategias de protección de microrredes en una arquitectura de red. Como consecuencia de lo anterior, también se presentan los objetivos planteados y además se expone la metodología propuesta para lograr la descripción de la estrategia seleccionada y su implementación dentro la arquitectura de red. Finalmente, se presentan los aportes del trabajo y una descripción del contenido de este documento.

1.1 Planteamiento del problema

En referencia a las estrategias de protección de microrredes es necesario reconocer que los sistemas eléctricos de potencia presentan condiciones de operación que pueden considerarse como normales o anormales, siendo esta última condición una representación de riesgo. Por lo general, con el fin de mantener el correcto funcionamiento del sistema y de los elementos que hacen posible el suministro de energía a la población, se utilizan esquemas de protección que contienen diversos dispositivos que se configuran de tal forma que cumplan funciones específicas dependiendo de su zona de influencia.

Con el incremento de la demanda de energía eléctrica en Colombia, que para enero de 2018 creció 3.5 porciento con respecto al mismo mes del año 2017 y a pesar de que se cuenta con una capacidad de generación de aproximadamente 40 porciento por encima de la demanda del país (Saavedra (2017)), (Rojas Pérez (2018)), por medio de la Ley 1715 de 2014 se busca promover el desarrollo y el uso de las fuentes de generación de energía eléctrica alternativas (*Energía Eléctrica - Ministerio de Minas y Energía* (n.d.)). Mediante esta ley se regula la integración de dichas fuentes al Sistema Energético Nacional que, en conjunto con la resolución CREG 030 de 2018, define los lineamientos para que los usuarios que

generen energía eléctrica puedan comerciar. De esta forma, se establecerán modificaciones sustanciales en la forma de operar y proteger a los sistemas de potencia (Ministerio de Minas y Energía (2018)).

Como consecuencia, se presentan algunas situaciones que se deben analizar desde el punto de vista de la protección de los sistemas eléctricos de potencia que consideran la denominada generación distribuida (GD). En este tipo de sistemas recaen una serie de retos en cuanto a su protección debido a que los dispositivos que cumplen esta tarea son diseñados para configuraciones radiales y flujos de carga unidireccionales. Así, con la instalación de GD en la red existente, pasarán a existir flujos bidireccionales y se presentará una pérdida de la coordinación de los dispositivos; lo que obliga a realizar reajustes al esquema de protección.

Para enfrentar los retos mencionados, surgen estrategias de protección que buscan integrar en su esquema los efectos mencionados para actuar de manera efectiva. Estas estrategias, se pueden dividir en tres grupos: a) esquemas que usan estrategias de optimización, los cuales intentan mantener el sistema de protección existente haciendo una coordinación de los elementos involucrados para obtener un óptimo en todos los posibles escenarios de conexión de la red utilizando diferentes métodos de optimización (Baghaee et al. (2018)),(Saleh et al. (2015)); b) técnicas adaptivas, que buscan implementar dispositivos de protección apoyados en medición de variables locales y toman decisiones para cambiar sus modos de operación según la conexión del sistema (Piesciorovsky & Schulz (2017)), (Muda & Jena (2017)); c) estrategias adaptivas basadas en comunicaciones las cuales, en su mayoría, dejan la responsabilidad de monitoreo de la red a un mando centralizado (observador global) que determina los cambios que se deben realizar en el sistema para actuar de manera correcta ante contingencias (Hatziargyriou (2014)), (Laaksonen et al. (2014)), (Ma et al. (2017)), (Zhang et al. (2019)), (Microgrids & Sidhu (2012)), (Ustun & Khan (2015)), (Ustun et al. (2011)) y (Liu et al. (2017)). Mientras que algunas estrategias como (Zamani et al. (2013)) plantean protecciones con mandos descentralizados para la protección del sistema.

La inclusión de estas tecnologías de protección basadas en comunicaciones incluye desafíos en cuanto al desarrollo de las redes inteligentes debido a la interacción e intercambio de información permanente entre sus dispositivos (Briefs & Energy (n.d.)). Incluir este tipo de sistemas a los ya existentes hace que la red a lo largo de la cadena de generación sea diversa y por lo tanto es difícil crear requisitos coherentes para cada una de las partes involucradas.

Por lo tanto, a través del mandato UE M/490 que busca realizar un trabajo para las redes inteligentes se desarrolla por medio de organizaciones de estandarización, un marco

que permite trabajar y mejorar metodologías que respalden estos procesos (CEN et al. (2014)). Para integrar gradualmente estos sistemas se tienen en cuenta tanto requisitos administrativos como de operación y las descripciones realizadas por medio de otras metodologías. Todo este procedimiento permitirá identificar brechas, por ejemplo, en las leyes del lugar donde se busca realizar la formalización de la estrategia de protección.

La implementación de una estrategia de protección es realizada por medio de estándares que determinan los pasos para describir estos sistemas y analizar los procedimientos que se realizan y los elementos que allí participan (CEN et al. (2014)). Para sintetizar, el enfoque principal de este documento será describir detalladamente un esquema de protección por medio del estándar IEC 62559-2 y asignarlo al modelo de arquitectura para redes inteligentes CEN-CENELEC-ETSI.

1.2 Objetivos

1.2.1 General

Desarrollar una estrategia de protección de microrredes dentro de una arquitectura de red identificando dispositivos, información intercambiada, requisitos operativos y regulaciones de importancia para su implementación.

1.2.2 Especificos

a) Analizar y discutir el estado actual de los sistemas de protección de microrredes.

b) Identificar y seleccionar estrategias de protección basadas em sistemas de comunicación.

c) Realizar una descripción de la estrategia seleccionada mediante el estándar IEC 62559-2.

d) Asignar la descripción realizada en las capas de interoperabilidad de la arquitectura de referencia para redes inteligentes.

e) Reportar el desarrollo de la arquitectura de referencia donde se evidencie el trabajo realizado para elaborar este trabajo.

1.3 Propuesta de trabajo

La propuesta de trabajo se enfoca en la descripción de cualquier estrategia de protección de microrredes para implementarla sobre un marco de referencia que hace parte de una

arquitectura de red.

Inicialmente, se realiza un estudio bibliográfico sobre las estrategias de protección de microrredes identificando las técnicas que más se utilizan. Estas técnicas por lo general son adaptivas que pueden usar o no comunicación entre sus dispositivos o basadas en métodos de optimización.

Posteriormente, se utiliza el estándar IEC 62559-2 como herramienta para la descripción de la estrategia seleccionada. Este estándar presenta una guía para detallar casos de uso especificando sus propiedades y funcionalidades de los dispositivos que interactúan. Por lo tanto, de la estrategia se extraerán y se mostrarán los actores que intervienen, la información que intercambian y los requisitos y regulaciones necesarias para su implementación divididos en siete pasos.

Finalmente, la información obtenida por medio del estándar permitirá desarrollar las capas de interoperabilidad de la arquitectura de referencia para redes inteligentes del grupo de estandarización CEN-CENELEC-ETSI. Allí se mostrarán los actores que intervienen, la información intercambiada, protocolos de comunicación, regulaciones y objetivos comerciales de la estrategia de protección seleccionada.

1.4 Aportes de la tesis

El principal aporte de este trabajo de grado es contribuir al entendimiento y comprensión de metodologías de estandarización de los procesos y sistemas, en este caso de microrredes eléctricas. Gracias al nivel de detalle propuesto en las metodologías, será posible determinar desde los dispositivos necesarios para lograr sistemas interoperables, hasta políticas que regulen la implementación de las estrategias de protección.

1.5 Publicaciones relevantes

Actualmente se encuentra en curso la redacción de un artículo que contiene los procedimientos y resultados del proyecto realizado. Este será enviado próximamente a una revista de relevancia en el campo de la ingeniería eléctrica.

1.6 Descripción del contenido de la tesis

El documento cuenta con seis capítulos que se explicarán en esta sección. En primer lugar, el capítulo introductorio relata la definición del problema, objetivos planteados, la propuesta de trabajo y los aportes de la tesis.

El segundo capítulo presenta los aspectos teóricos útiles para comprender la metodología y el desarrollo de la propuesta. Allí se hace énfasis en definir conceptos utilizados a lo largo de los capítulos 3 y 4 como arquitectura, marco SGAM, interoperabilidad, control centralizado y descentralizado, caso de uso y estrategias de protección.

El capítulo 3 contiene la metodología propuesta para desarrollar la arquitectura de protección donde se plantean tres pasos: análisis y selección de la estrategia de protección, descripción y desarrollo dentro de una arquitectura de referencia.

Luego, en el capítulo 4 se aplica la metodología y se muestra el trabajo realizado durante la selección, descripción y desarrollo de la estrategia de protección en las zonas y dominios del marco SGAM.

En el capítulo 5 se mencionan las conclusiones que se obtienen como consecuencia del trabajo realizado y se hacen algunas recomendaciones de utilidad para continuar con el trabajo realizado, referente a las temáticas que no fueron estudiadas en este documento.

Capítulo 2

Aspectos teóricos básicos

Este capítulo muestra los conceptos básicos que se consideran importantes para comprender la metodología y el desarrollo específico que se presentan en los capítulos 3 y 4. Los detalles específicos se presentan en las referencias asociadas.

2.1 Arquitectura de referencia

Según (CEN et al. (2014)), una arquitectura de red es un conjunto de propiedades de un sistema que describe los elementos, las relaciones existentes y las técnicas o principios en los que se basa su diseño. Está contenida dentro de un dominio específico denotado por un marco de referencia.

2.1.1 Marco de referencia SGAM (Smart Grid Architecture Model)

El marco de referencia ofrece las pautas para diseñar casos de uso de redes inteligentes representados desde el punto de vista de la interoperabilidad que servirán para implementar elementos a la red eléctrica (CEN et al. (2014)). Es un marco tridimensional compuesto por dominios, zonas y cinco capas de interoperabilidad: negocio, función, información, comunicación y componentes, tal como se presenta en la figura 2.1.

2.1.1.1 Dominios

Se define como un marco detallado de operación acotado entre la cadena de generación: generación, transmisión, distribución, DER y consumidores (CEN et al. (2014)).

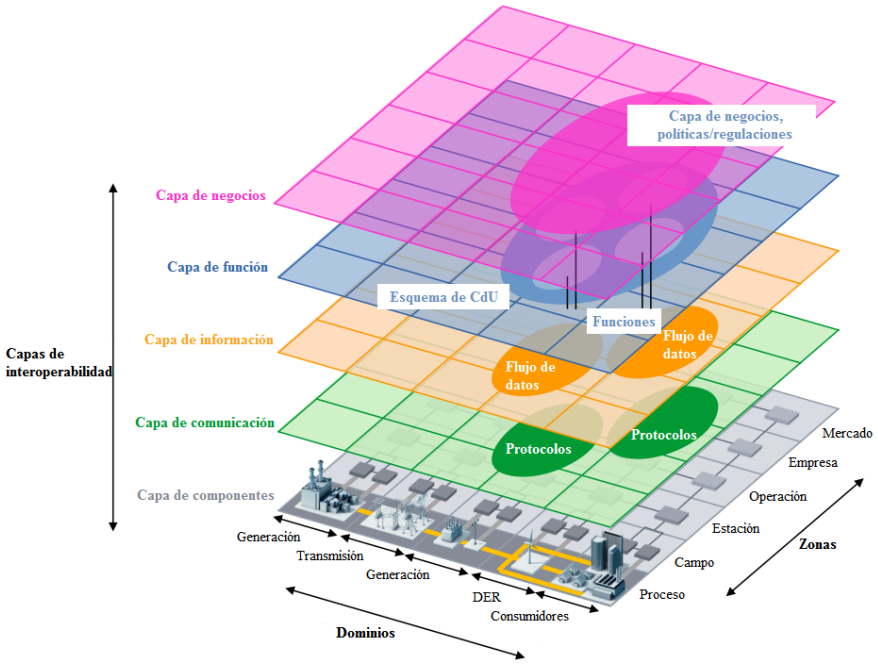

Figura 2.1. Dominios y zonas del marco SGAM

2.1.1.2 Zonas

Representan los niveles administrativos del sistema, divididos en seis partes: proceso, campo, estación, operación, empresa y mercado (CEN et al. (2014)).

2.1.1.3 Ubicación de dispositivos en las zonas del marco SGAM

Los dispositivos participantes en un sistema que interactúa dentro del marco SGAM están ubicados en zonas específicas y deben cumplir lo presentado en la tabla 2.1.

2.1.1.4 Capas de interoperabilidad

Es una propiedad que permite a diversos componentes o sistemas, trabajar juntos por un propósito específico. (*IEC 60050 - International Electrotechnical Vocabulary - Welcome* (n.d.))

Por su parte, (CEN et al. (2014)) define la interoperabilidad como a la capacidad de dos o más elementos para intercambiar información utilizada para una cooperación correcta.

Zona	Descripción
Proceso	Se incluyen transformaciones de energía (electricidad, solar, calor, agua, viento) y los equipos directamente involucrados. (generadores, transformadores, líneas aéreas, cables, cargas eléctricas de cualquier tipo de sensores y actuadores que estén conectados directamente o al proceso).
Campo	Incluyendo equipos de protección que controlan y monitorean el proceso del sistema de energía como relés de protección, cualquier tipo de dispositivo electrónico inteligente que adquiera y use datos del proceso.
Estación	Elementos donde exista concentración de datos, agregación funcional, automatización de subestaciones, sistemas SCADA locales, supervisión de planta.
Operación	Sistemas de administración de distribución (DMS), sistemas de administración de energía (EMS), sistemas de generación y transmisión, sistemas de administración de micro rredes, (DER), vehículo eléctrico (EV) con sistemas de recarga.
Empresa	Incluye procesos comerciales y organizativos, servicios e infraestructuras para empresas (empresas de servicios públicos, proveedores de servicios, comercializadores de energía), por ejemplo, gestión de activos, logística, formación del personal, gestión de relaciones con el cliente, facturación y beneficios económicos.
Mercado	Reflejando las operaciones de mercado posibles a lo largode la cadena de generación, por ejemplo, comercio de energía, mercado mayorista, mercado minorista.

Tabla 2.1. Ubicación de dispositivos en zonas del marco SGAM.

2.2 Control centralizado y descentralizado

2.2.1 Control centralizado

En un sistema de control centralizado la responsabilidad de tomar decisiones, maximizar u optimizar algún proceso recae en un operador de sistema central (Hatziargyriou (2014)).

En (Quintanilla & Yarza (2010)) se define un sistema centralizado como un esquema en el que existe un elemento central y decide sobre los dispositivos de protección realizando configuraciones para diferentes topologías de operación.

2.2.2 Control descentralizado

CEN et al. (2014)) define un sistema descentralizado como aquel en el que los participantes cambian permanentemente sus roles e interactúan cooperativamente para generar información.

Por su parte (Quintanilla & Yarza (2010)) menciona que es un esquema de control que no requiere de un dispositivo central debido a que la inteligencia está repartida entre las

protecciones que lo componen. De esta forma cada dispositivo es autónomo para realizar su ajuste dependiendo de la información que recibe.

2.3 Caso de uso

Los autores (Enanv et al. (2010)) y (Gottschalk et al. (2017)) coinciden en que un caso de uso es una descripción de las acciones que realiza un sistema y produce un resultado observable. Por su parte (Ref 4) define un caso de uso como una especificación de una serie de acciones que un sistema o cualquier otra entidad puede realizar interactuando con los actores presentes.

2.3.1 Actor

Un actor es un elemento dentro del sistema que interactúa y se comunica con otros elementos (Specification (2013)).

2.3.2 Escenario

El escenario es una secuencia de interacciones o eventos causados por la actividad de un actor (Enanv et al. (2010)).

2.3.3 Evento

Suceso que es desencadenado por la acción de un actor y que hace parte del desarrollo del escenario.

2.4 Estrategia de protección

Es un sistema responsable de proteger adecuadamente una microrred ante fallas que se presente (Shiles et al. (2018)). Las estrategias de protección utilizan técnicas que pueden ser: adaptivas, adaptivas que emplean comunicación o basadas en optimización.

2.4.1 Estrategia de protección adaptiva

En este tipo de estrategia las protecciones monitorean las condiciones de la red para verificar que sus ajustes son los correctos para cada modo de operación. En caso de que usen un sistema de comunicaciones, el control de la arquitectura puede ser centralizado o descentralizado (Quintanilla & Yarza (2010)).

2.4.2 Estrategia de protección basada en optimización

El enfoque de optimización utiliza un conjunto de posibles escenarios de falla para configurar los dispositivos de protección ante todos los casos posibles de configuración de red (Behnke et al. (2018)).

Capítulo 3

Metodología propuesta para el desarrollo de la arquitectura de protección

Con base en la evolución actual de las redes inteligentes se tiene en cuenta los requerimientos de las nuevas tecnologías para describir por completo su funcionamiento. Por lo tanto, para desarrollar un problema genérico de protección de microrredes, descrito por medio del estándar IEC 62559 y posteriormente la descripción del mismo en una arquitectura de referencia, requiere la elaboración de una metodología.

La figura 3.1 muestra la metodología propuesta para el desarrollo de la arquitectura de protección de microrredes.

La metodología propuesta en la figura 3.1 se divide en cuatro etapas que se presentan a continuación:

3.1 Etapa 1: Análisis y selección de la estrategia de protección

En esta etapa se realiza una investigación y análisis documental para seleccionar la estrategia de protección que se describe dentro de la arquitectura de referencia. Esta etapa se divide en 4 pasos que se presentan a continuación:

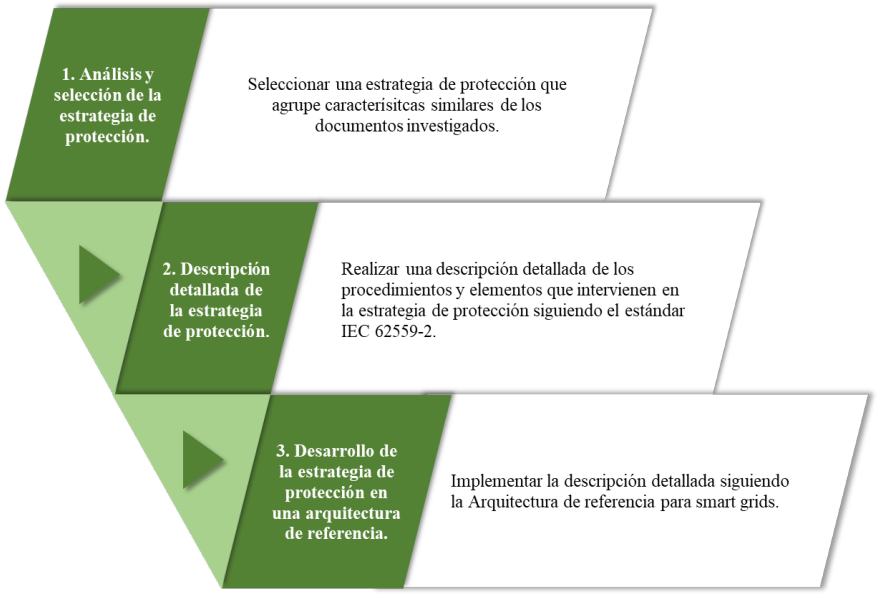

Figura 3.1. Metodología propuesta para el desarrollo de la arquitectura de protección de microrredes

3.1.1 Paso 1: Análisis de la bibliografía de referencia

El tema de protección de microrredes ha sido ampliamente tratado en varias referencias, tal como se muestra en el capítulo 1. A partir del análisis de la bibliografía citada, se debe seleccionar las técnicas de protección más relevantes y que tengan la mayor relación posible al tema de investigación. Esto se refiere a las técnicas utilizadas para desarrollar las estrategias de protección que por lo general son de optimización, adaptivas o basadas en comunicaciones.

3.1.2 Paso 2: Identificación de características generales de la estrategia de protección

Filtrar la información más relevante para la investigación requiere un análisis adicional sobre las características generales de la estrategia de protección de microrredes que se está investigando. Estas características hacen referencia a las técnicas y dispositivos de protección en las que los autores fundamentan el funcionamiento de las estrategias. Por lo tanto, al identificar estas características se encontrarán similitudes entre los documentos analizados.

3.1.3 Paso 3: Selección de la estrategia de protección

Con la información obtenida en los pasos 1 y 2 es posible seleccionar una estrategia de protección que agrupe la mayor cantidad posible de características identificadas. De esta forma, la estrategia seleccionada estará contenida en las técnicas y dispositivos utilizados comúnmente.

3.1.4 Paso 4. Análisis del funcionamiento de la estrategia de protección

Un análisis del funcionamiento de la estrategia seleccionada permitirá identificar los elementos que interactúan e intercambian información para llevar a cabo las funcionalidades de la estrategia. Además, servirá como referencia para realizar una descripción detallada en la sección 3.2.

3.2 Etapa 2: Descripción de la estrategia de protección

Los pasos descritos hasta este punto entregan las herramientas necesarias para continuar con la etapa 2 de la metodología propuesta, dividida en 4 pasos. Esta etapa se desarrolla siguiendo el estándar IEC 62559-2 que plantea una guía para la descripción de sistemas que pretenden ser desarrollados dentro de una arquitectura de referencia. El estándar plantea una plantilla de caso de uso estándar que especifica detalladamente las acciones que realiza un sistema siguiendo los pasos que se muestran a continuación:

- Describir de forma general el caso de uso.
- Realizar diagramas del caso de uso.
- Especificar detalles técnicos.
- Analizar paso a paso el caso de uso.
- Identificar la información que se intercambia entre actores.
- Definir los requisitos necesarios para hacer efectiva la comunicación (opcional).
- Definir términos y definiciones comunes.

El desarrollo de las secciones opcionales se deja en consideración de quien va a describir el caso de uso, puesto que las funciones que caracterizan el sistema determinan la necesidad de que sean desarrolladas.

La plantilla del estándar IEC 62559-2 recopila toda la información de estos pasos en tablas que se mostrarán en el capítulo 4 de este documento.

3.2.1 Paso 1: Describir de forma general el caso de uso

La ejecución de este paso comprende siete secciones que recopilan datos generales del caso de uso, que son:

3.2.1.1 Nombre del caso de uso

En esta sección se le entrega un ID al caso de uso y un nombre relacionado a las funciones que realiza. También debe asignársele una ubicación dentro de los dominios y zonas del marco SGAM.

3.2.1.2 Administración de versiones

La administración de versiones debe contener un número en orden consecutivo de los cambios que se realizan en el caso de uso, además de la fecha en que se realiza el cambio, el nombre de la(s) persona(s) que hace(n) el cambio y su estado actual que se especifica como: borrador, actualización o definitivo.

3.2.1.3 Alcance y objetivos del caso de uso

Se plantean los objetivos propuestos que motivaron la descripción detallada del caso de uso de forma puntual, antecedidos de un titular breve. El alcance describe los objetivos planteados y los límites que puede tener el caso de uso en un texto corto y preciso. La última parte de la tabla hace referencia a los casos de negocio relacionados y las restricciones o leyes que afecten la implementación del caso.

3.2.1.4 Narrativa del caso de uso

Esta sección describe el problema de dos formas: breve y completa. La descripción breve no debe contener más de diez líneas y la descripción completa contiene más detalle desde el punto de vista de un usuario, donde se menciona cómo sucede cada actividad dentro del funcionamiento. Las descripciones se realizan de forma que facilite su comprensión, incluso para personas ajenas al proyecto.

3.2.1.5 Indicadores clave de rendimiento

Los indicadores de rendimiento tienen relación a los objetivos planteados y hacen referencia a los beneficios de implementar el caso de uso. Cada indicador debe tener un ID único, un nombre, una descripción y el objetivo al cual está sujeto.

3.2.1.6 Condiciones del caso de uso

Esta sección plantea la posibilidad de que existan un número determinado de suposiciones sobre las condiciones o configuraciones del caso de uso, acompañadas de un requisito que debe cumplirse para que los escenarios se completen con éxito. Por lo general se relacionan directamente con los actores y los eventos del sistema. Cada suposición y requisito previo requerirá una tabla para su descripción.

3.2.1.7 Información adicional sobre el caso de uso para clasificación/mapeo

La información adicional restante se recopila en este paso e incluye:

Relación con otros casos de uso: En caso de que existan desarrollos similares en la temática de protección de microrredes, la relación con los otros casos de uso se especifica con tres posibles enlaces:

Incluido: Se refiere a que el caso de uso que se está desarrollando está contenido dentro de otro caso de uso con límites más amplios.

Extendido: Hace referencia a una descripción más detallada de otro caso de uso que ya ha sido reportado.

Asociado: El caso de uso puede unirse a otro para conformar un caso de uso más grande.

Nivel de profundidad: Refleja el grado de especialización del caso de uso que por lo general son: alto nivel, genérico, detallado o especializado.

Priorización: El caso de uso debe calificarse desde muy importante hasta obligatorio u opcional. Esto es acordado por las personas que realizan la descripción.

Relación genérica, regional o nacional: La aplicación del caso de uso debe especificarse en caso de que pueda realizarse en cualquier parte o en sitios específicos.

Naturaleza del caso de uso: Describe el campo de atención del caso de uso como técnico, político, negocio, mercado, prueba, etc.

Otras palabras clave para la clasificación: Palabras o frases con las que también se puede relacionar el caso de uso.

3.2.1.8 Observaciones generales

Las observaciones que sean necesarias mencionar y que no encajan en otra categoría de la descripción de la sección 3.2.1 se insertan aquí separadas por viñetas.

3.2.2 Paso 2: Realizar diagrama del caso de uso

El diagrama del caso de uso debe contener los actores y escenarios existentes y especifica su interacción por medio de líneas de conexión. Los actores mostrados en el diagrama deben coincidir con elementos clasificados en la sección 3.2.3.1 y los escenarios se ajustan a lo desarrollado en 3.2.4.1. Cualquier tipo de dibujo que represente estos elementos del sistema es permitido.

3.2.3 Paso 3: Especificar detalles técnicos

Los detalles técnicos incluyen dos categorías tabuladas, que definen los actores y especifican las referencias bibliográficas consultadas para el desarrollo del caso de uso, así:

3.2.3.1 Actores

Los actores se pueden clasificar en grupos según sus propiedades, con tantos grupos como se considere necesario. La tabla contiene el nombre del grupo, una definición o descripción, una lista de los actores que están incluidos, el tipo de actor (persona, sistema, base de datos, organización o dispositivo) y una corta descripción. Si se tienen datos adicionales que no puedan ser colocados en la descripción, se añaden en la información específica del caso de uso. Cada agrupamiento requiere la construcción de una tabla.

3.2.3.2 Referencias

En esta tabla se enumeran las referencias consultadas y de utilidad en el caso de uso incluyendo las que fueron consultadas en la sección 3.1. La información requiere un nombre, el tipo de referencia (artículo, sitio web, etc.), referencia, estado (inicial, final, volumen, etc.),

se especifica el impacto de la referencia en el caso de uso (bajo, medio alto), autores de la referencia y un link de ser necesario.

3.2.4 Paso 4: Analizar paso a paso el caso de uso

El análisis paso a paso del caso de uso ayudará a describir con detalle las actividades que se presentan especificando actores, eventos y escenarios. Esta parte es una asociación a la narrativa realizada en la sección 3.2.1.4 y debe tener una relación directa con el diagrama del caso de uso desarrollado en la sección 3.2.2. Cada paso describe una comunicación o actividad entre los actores listados en la sección 3.2.3.1. El análisis está dividido en dos partes, como se muestra a continuación:

3.2.4.1 Resumen de escenarios

En esta sección se tabulan los escenarios que existen dentro del caso de uso en orden de ejecución. Generalmente se enumeran primero los escenarios normales, es decir, aquellos que no representan una falla. La tabla contiene la numeración en orden ascendente, nombre, descripción completa y el actor que hace que el escenario se ejecute, el evento que desencadena, la condición previa para que el actor ejecute su actividad y el evento posterior que da paso a las demás actividades que componen el escenario.

3.2.4.2 Pasos-escenarios

En esta sección es necesario introducir el nombre del escenario que se va a describir, numerar el orden de ejecución de las actividades, el evento y por último el nombre y una descripción del proceso que se está llevando a cabo. El evento siguiente es activado por el que acaba de terminar y cada uno de ellos se describe de la misma forma hasta que el escenario cumpla su función y pueda volver a iniciarse. El procedimiento se realiza para cada escenario existente en el caso de uso.

La segunda parte de la tabla caracteriza el tipo de señal producida por un actor, se especifica el actor que produce la información, el que recibe esta información, la información intercambiada entre actores presentada en la sección 3.2.5 y algunos requisitos establecidos que se mostrarán en la sección 3.2.6. El tipo de señal que un actor produce puede clasificarse así:

Obtener (predeterminado): El actor receptor obtiene una información después de solicitarla al productor.

Crear: El actor productor crea un elemento de información y lo envía al receptor.

Cambiar: El actor productor actualiza la información contenida el receptor.

Borrar: El productor de información borra la información del receptor.

Cancelar / cerrar: Un proceso ha terminado.

Ejecutar: Una acción o servicio es realizada.

Informar: El actor que produce la información entrega información de datos almacenados.

Temporizar: Si un actor hace las veces de productor y receptor debe tener un tiempo de espera.

Repetir: Se realizan acciones de intercambio hasta satisfacer una condición definida en algún evento.

El productor y el receptor de la información son los actores de la sección 3.2.3.1.

3.2.5 Paso 5: Identificar la información que se intercambia

Esta sección hace referencia a la información intercambiada entre actores, proporcionándoles una característica particular de la información (enviar, almacenar, informar, actualizar, etc.). Adicionalmente, la tabla debe contener un ID específico, una breve descripción y requisitos (de ser necesario) de la información intercambiada mostrados en la sección 3.2.6 para que el proceso se cumpla.

3.2.6 Paso 6: Definir los requisitos necesarios para hacer efectiva la comunicación (opcional)

Generalmente estos requisitos pretenden proteger, almacenar o cifrar correctamente los datos que se manejan dentro del caso de uso. Se clasifican en categorías asignándoles un ID, un nombre único y una breve descripción. Luego, a cada requisito se le asigna un ID que se relaciona con el ID de su categoría y posteriormente adquieren un nombre y una descripción.

3.2.7 Paso 7: Definir términos y definiciones comunes

Contiene términos y definiciones comunes que se han utilizado a lo largo de la descripción del caso de uso, organizados en un glosario.

3.3 Etapa 3: Desarrollo de la estrategia de protección en una arquitectura de referencia

La etapa 3 de la metodología propuesta muestra cómo asignar un caso de uso al marco de referencia SGAM desarrollado en (CEN et al. (2014)). Es importante reconocer en qué dominios y zonas del marco realiza sus funciones para desarrollar correctamente las capas. Estas capas son una representación dentro del marco SGAM que buscan que el sistema sea interoperable.

El desarrollo de la estrategia de protección en la arquitectura está compuesto por cinco pasos que se muestran a continuación:

3.3.1 Paso 1: Desarrollo de la capa de componentes

El desarrollo de esta capa se deriva del diagrama del caso de uso realizado en la sección 3.2.2 que muestra los actores y escenarios de la estrategia de protección. Debido a que el diagrama del caso de uso es un dibujo libre, los actores se deben llevar a una representación técnica que muestre la comunicación existente entre ellos. Tanto los actores como los escenarios se ubican en los dominios y zonas apropiados y será la base para desarrollar las cuatro capas siguientes.

3.3.2 Paso 2: Desarrollo de la capa de negocios

Aquí se mencionan los objetivos comerciales y las restricciones económicas y regulatorias del caso de uso. Esta información está definida en los alcances y objetivos de la sección 3.2.1.3. Las restricciones y limitaciones mencionadas deben tenerse en cuenta como requisitos funcionales para su implementación.

3.3.3 Paso 3: Desarrollo de la capa de función

La capa de función está diseñada para representar las actividades de los actores dentro de los escenarios, ubicándolos en los dominios y zonas adecuados. La relación entre actores y escenarios se deriva de la segunda parte de la tabla referente a los pasos-escenarios

desarrollados en la sección 3.2.4.2. Una vez ubicados, se representa mediante líneas de conexión los actores que intervienen en el desarrollo de los escenarios.

3.3.4 Paso 4: Desarrollo de la capa de información

Esta capa representa la información que se utiliza y se intercambia entre los actores del caso de uso, contenida en la sección 3.2.5. Esta información debe mostrarse de forma escrita sobre las flechas que representan la comunicación.

3.3.5 Paso 5: Desarrollo de la capa de comunicación

Su énfasis es describir los protocolos que se utilizan para el intercambio de la información entre los actores del caso de uso. Deben ilustrarse mencionando el estándar que describe los protocolos que hacen efectiva la comunicación.

Capítulo 4

Desarrollo de la arquitectura de protección

En este capítulo ejecuta la descripción de una estrategia de protección de microrredes dentro de una arquitectura de referencia siguiendo la metodología mencionada en el capítulo 3. Las etapas que serán presentadas a continuación mostrarán la selección de la estrategia de protección, su descripción por medio de la metodología IEC 62559-2 y finalmente el desarrollo de las capas de interoperabilidad dentro del marco SGAM.

4.1 Etapa 1: Análisis y selección de la estrategia de protección

A partir de la metodología propuesta en el capítulo 3, en este capítulo se presenta la selección de una estrategia de protección que agrupe las características descritas en las etapas de la sección 3.1. La técnica seleccionada cuenta con protecciones adaptivas, basada en comunicaciones y con mandos centralizados. La estrategia presentada en (Hatziargyriou (2014)) describe un sistema adaptivo basado en ajustes calculados en tiempo real que se ilustra en la figura 4.1

El sistema de protección cuenta con dos bloques: bloque en tiempo real y bloque en tiempo no real. El bloque en tiempo real permite el análisis del estado actual de la microrred a partir de mediciones periódicas entregadas por medidores inteligentes. Estas mediciones son comparadas con las condiciones predefinidas de la red por un relé multifuncional que actúa como protección centralizada. Este relé detecta las perturbaciones mediante las características de disparo ajustadas en los dispositivos de protección y, cuando se detecta una condición de falla, envía una señal de disparo a los interruptores de la zona afectada.

Cuando ocurre una falla, el relé multifuncional se comporta como un relé convencional que tiene control sobre varios interruptores automáticos, pero limita su aplicación a una zona específica de la red.

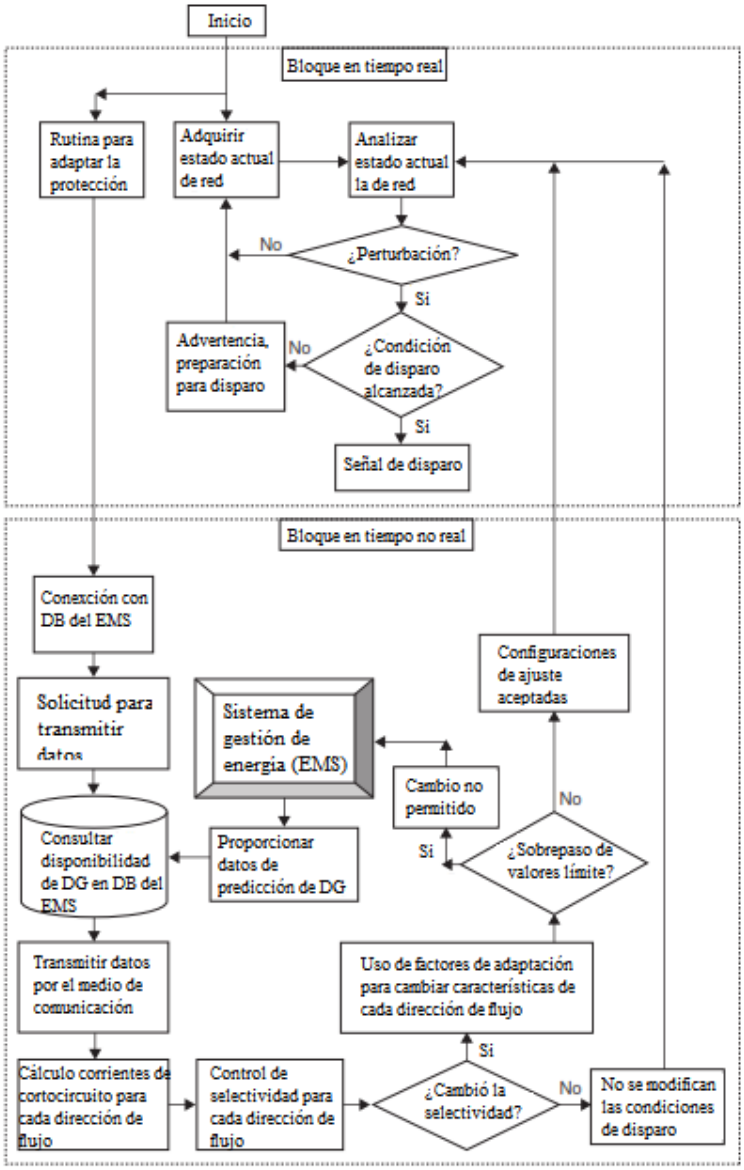

Figura 4.1. Diagrama de flujo del esquema de protección seleccionado. Tomado de (Hatziargyriou (2014))

El bloque en tiempo no real utiliza los datos de predicción de disponibilidad de las fuentes de generación distribuida (DER) a través de un sistema de gestión de energía (EMS), el cual almacena la información en una base de datos (DB). Esta información se utiliza para conectar o desconectar DER que pueden generan un cambio en la topología de la microrred, por lo tanto, es necesario realizar un control de selectividad. Este control es efectuado por el relé para verificar que las condiciones límite predefinidas por el sistema no sean sobrepasadas cuando se presenta un cambio de topología. La función del relé multifuncional, en este caso, es adaptar las funciones de protección para la nueva topología de red y sí las condiciones límites del sistema no se superan, entonces se acepta la nueva topología. Cuando el cambio se realiza, la base de datos informa mediante sus servidores la información de los parámetros de interés al relé multifuncional con los cuales se reajustan las protecciones donde sea necesario. Si no existe una forma de adaptar las protecciones sin violar las condiciones límite, el relé envía una señal que prohíbe la acción prevista por el EMS. De manera similar se realiza el cambio de topología cuando la red está conectada y entrará en operación en modo isla, aquí, la base de datos provee al relé las contribuciones de corrientes de cortocircuito cuando ocurre el cambio. Por lo tanto, el relé supervisa continuamente la disponibilidad de las DER y de la red principal para realizar el procedimiento cuando corresponda.

Todo el proceso de adaptación realizado por el relé y demás elementos que contribuyen en la actividad, está limitado por la probabilidad de que ocurra una falla durante el análisis, por lo tanto, el cambio debe tardar pocos segundos.

4.2 Etapa 2: Descripción de la estrategia de protección

Siguiendo la plantilla propuesta en el estándar IEC 62559-2 desarrollada en la sección 3.2, se realiza la descripción detallada del caso de uso. A continuación, se muestran las tablas correspondientes al desarrollo del caso de uso llamado “Estrategia de protección de microrredes basado en sistemas de comunicación”. Estas tablas muestran los resultados que tienen más relevancia en el desarrollo de la arquitectura; por lo tanto, algunos elementos de la descripción detallada podrán encontrarse en los anexos de este documento.

4.2.1 Paso 1: Describir de forma general el caso de uso

En la sección 3.2 se definen los alcances, objetivos, los casos de negocio relacionados y las restricciones existentes para la implementación de la estrategia de protección mostrados en la tabla 4.1. El resto de los pasos que se desarrollan en esa sección estarán ubicados en la sección A.1 de los anexos.

Alcance y objetivos del caso de uso.	
Alcance	Considerando la evolución de las redes de distribución y el resto de actores de la cadena de generación los cuales están experimentando cambios en su estructura, es necesario hacer cambios en las estrategias de protección que se utilizan actualmente. Las estrategias de protección basadas en comunicaciones para estas nuevas estructuras de red (microrredes) deben ser capaces de despejar selectivamente las fallas para mitigar los efectos que puedan generar a lo largo de la red. Estas estrategias permitirán tener un mayor control sobre la red eléctrica entregando beneficios operacionales como el monitoreo constante de la red con informes actualizados de la red. Por lo tanto, una buena configuración y manejo de las protecciones permitirá que las fuentes de energía distribuida operen sin inconvenientes cuando entren en operación y generen un cambio en la topología de la red, maximizando el uso y la capacidad de los activos de generación y como consecuencia lograr un sistema más eficiente. Una microrred operada y protegida de forma correcta permitirá finalmente que el suministro de energía y el sistema en general sea confiable, seguro y continuo.
Objetivos	• Mitigar el efecto de las fallas. • Obtener beneficios operacionales. • Maximizar el uso y capacidad de los activos de generación. • Incrementar eficiencia. • Mejorar la continuidad del servicio.
Casos de negocio relacionados	• Operación de la microrred de distribución. • Estabilidad de la microrred. • Protección de la microrred. • Mejoramiento de los índices de continuidad del suministro.

Tabla 4.1. Alcance y objetivos del caso de uso

4.2.2 Paso 2: Realizar diagrama del caso de uso

A partir de los actores y escenarios identificados en la descripción se realiza el diagrama de la estrategia de protección que se ilustra en la figura 4.2.

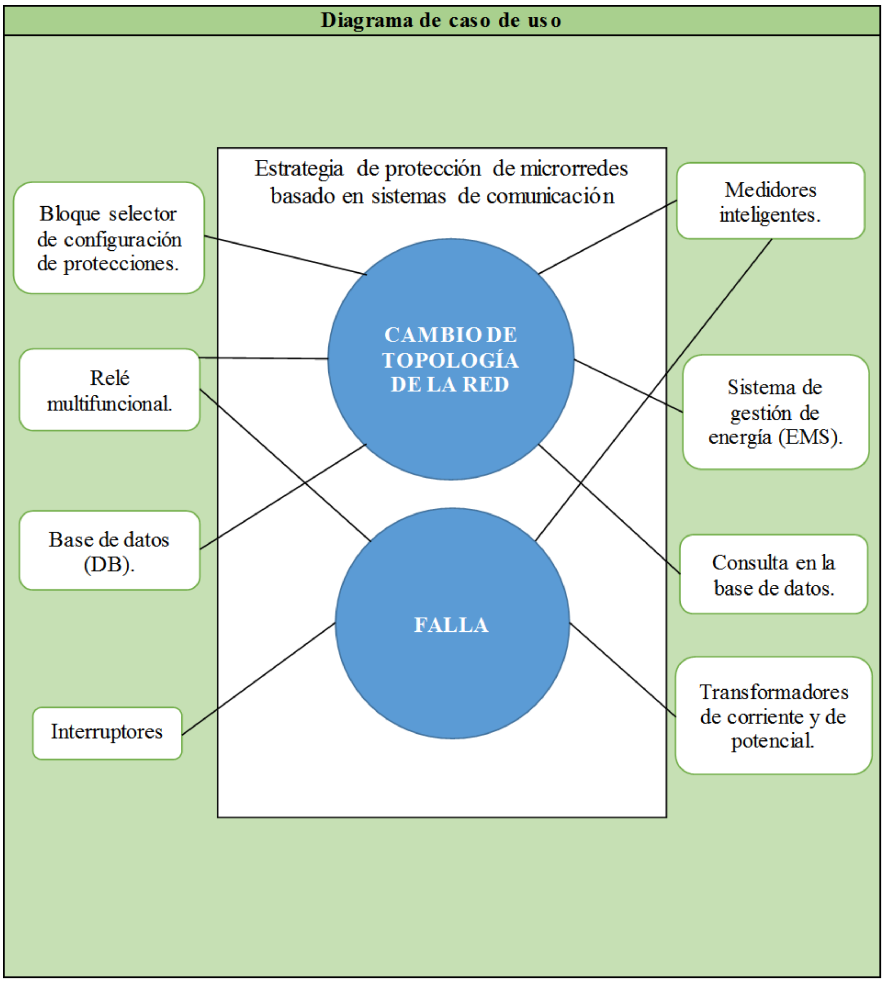

Figura 4.2. Diagrama del caso de uso

4.2.3 Paso 3: Especificar detalles técnicos

Los actores fueron clasificados en cuatro grupos: medidores, sensores, actuadores y otros actores. Estas clasificaciones se mostrarán de la tabla 4.2 a la 4.5, respectivamente.

Actores			
Agrupamiento		**Descripción del grupo**	
Medidores		Dispositivo destinado a ser utilizado para realizar mediciones, solo o en combinación con dispositivos adicionales. (Véase IEC electropedia: Instrumento de medición).	
Nombre del actor	**Tipo de actor**	**Descripción del actor**	**Más información específica de este caso de uso**
Medidores inteligentes	Sistema	Conjunto de dispositivos que monitorean el estado de la microrred recibiendo y enviando información sobre los cambios de esquema o eventualidades que se puedan presentar en ella.	El intercambio de información en tiempo real se hará siguiendo los protocolos descritos en el estándar IEC 61850.

Tabla 4.2. Actores: agrupación de medidores

Agrupamiento		**Descripción del grupo**	
Sensores		Parte de un instrumento de medición, o cadena de medición, que está directamente afectada por la medida y que genera una señal relacionada con el valor de la medida. (Véase IEC electropedia: Sensor).	
Nombre del actor	**Tipo de actor**	**Descripción del actor**	**Más información específica de este caso de uso**
Transformadores de corriente y potencial	Sistema	Dispositivos encargados de reducir la corriente y tensión en la microrred con el fin de permitir el empleo de los sistemas de medición y protección adecuadamente.	El intercambio de información en tiempo real se hará siguiendo los protocolos descritos en el estándar IEC 61850.

Tabla 4.3. Actores: agrupación de sensores

Los grupos de medidores y sensores tienen un solo elemento dentro de su composición

debido a que son sistemas que están compuestos por varios dispositivos en la microrred.

Agrupamiento		**Descripción del grupo**	
Actuadores		Dispositivo que realiza un movimiento cuando es excitado por una señal eléctrica (Véase IEC electropedia: Actuador).	
Nombre del actor	**Tipo de actor**	**Descripción del actor**	**Más información específica de este caso de uso**
Relé multifuncional	Sistema	Elemento inteligente que genera señales de disparo cuando recibe una señal eléctrica proveniente de la red o desde el mismo equipo.	Al tener control central, se considera un solo relé que controla una cantidad limitada de interruptores.
Interruptor	Dispositivo	Dispositivo que recibe una señal eléctrica de disparo proveniente de un relé multifuncional.	
Bloque selector de configuración de protecciones	Sistema	Sistema que evalúa las nuevas condiciones de operación a causa de la integración de nuevas fuentes de generación distribuida.	
Sistema de gestión de energía (EMS)	Sistema	El sistema de gestión de energía se encarga de conectar o desconectar fuentes de generación distribuida proporcionando datos de predicción de disponibilidad de las mismas almacenados en la base de datos.	

Tabla 4.4. Actores: agrupación de actuadores

Las referencias de utilidad para el desarrollo de la descripción de la estrategia de protección estarán tabuladas en la sección A.1 de los anexos.

Agrupamiento		**Descripción del grupo**	
Otros actores		Cualquier cantidad de elementos que no clasifican como medidor, sensor o actuador dentro del sistema.	
Nombre del actor	**Tipo de actor**	**Descripción del actor**	**Más información específica de este caso de uso**
Base de datos (DB)	Base de datos	En las bases de datos se almacena la configuración real de la red y los datos sobre los recursos de generación distribuidos.	Los datos que se almacenan deben ser protegidos para evitar la manipulación de terceros.
Consulta en la base de datos	Dispositivo	Elemento encargado de consultar a la base de datos la disponibilidad de los recursos de generación distribuida.	

Tabla 4.5. Actores: agrupación de otros actores

4.2.4 Paso 4: Analizar paso a paso el caso de uso

Una vez definidos los actores, se describen los escenarios de la estrategia de protección de microrredes basada en sistemas de comunicación. De la estrategia estudiada se enumeran dos escenarios posibles: cambio de topología de la red y falla.

Para el escenario de cambio de topología el actor primario es el EMS debido a que en el momento en que recibe los datos de predicción de las DER, se inicia el proceso de cambio de topología.

Condiciones del escenario						
No.	**Nombre del escenario**	**Descripción del escenario**	**Actor primario**	**Evento desencadenante**	**Condición previa**	**Condición siguiente**
1	Cambio de topología de la red	El sistema utiliza los datos de predicción de disponibilidad de las fuentes de generación distribuida para conectar o desconectar los recursos según estos datos almacenados. Después realiza un control de selectividad que estima las corrientes de cortocircuito para cada dirección de flujo de la microrred, adaptando los elementos de protección en consecuencia. Si existe una adaptación exitosa, significa que las condiciones límite del sistema no se violan y las características de disparo de los relés serán apropiadas. En caso de que no haya una solución posible que no viole estas condiciones, se generará una señal que prohíbe la conexión o desconexión de las fuentes.	Sistema de gestión de energía (EMS)	Predicción para conectar o desconectar una fuente de generación distribuida.	La base de datos proporciona información necesaria de disponibilidad	Cambio de topología permitido o no permitido

Tabla 4.6. Visión general de escenarios: cambio de topología de la red

Por su parte el escenario de falla inicia la ejecución del procedimiento cuando los transformadores de corriente y de potencial envían una señal, que inicia un análisis de verificación si los datos se traducen en una falla.

Condiciones del escenario						
No.	**Nombre del escenario**	**Descripción del escenario**	**Actor primario**	**Evento desencadenante**	**Condición previa**	**Condición siguiente**
2	Falla	La microrred es monitoreada constantemente con los datos que se originan desde los equipos de medida y la red y, cuando algún cambio de topología es aceptado, significa que las protecciones están adaptadas para actuar ante cualquier evento de falla que se presente. De acuerdo a estas nuevas características de protección y las señales de medición entregadas por los transformadores de potencial y de corriente, el relé multifuncional decide si existe falla o no enviando la señal a los respectivos interruptores.	Transformadores de corriente y de potencial	Detección de condición de disparo	El relé multifuncional recibe y compara la información suministrada por los medidores inteligentes y los transformadores de corriente y de potencial.	Apertura de interruptores en las zonas afectadas por la falla.

Tabla 4.7. Visión general de escenarios: falla

Los escenarios se analizan son detallados a partir de la acción de un actor principal que desencadena una serie de eventos para cumplir el escenario totalmente. Para el escenario de cambio de topología de la red se tienen nueve pasos, mientras que en el escenario de falla se identifican cinco eventos. Estos pasos se presentan en las tablas 4.8 y 4.9 para el cambio de topología y en la tabla 4.10 para falla.

Escenario			
Nombre del escenario		**Cambio de topología de la red**	
No.	**Evento**	**Nombre del proceso/actividad**	**Descripción de proceso/actividad**
1	Medición continua de parámetros de la microrred.	Monitoreo del estado actual de la red.	Los medidores inteligentes envían constantemente la información captada a los relés multifuncionales que monitorean la red.
2	Almacenamiento de datos de DER y de configuraciones de la red en la base de datos.	Preparación de disponibilidad de fuentes de generación distribuidas.	El sistema de gestión de energía (EMS) proporciona datos de predicción sobre la disponibilidad de las fuentes de energía distribuida y las posibles configuraciones de la red, almacenando esta información en las bases de datos.
3	La base de datos (DB) envía datos almacenados y configuraciones de red.	Comunicación continua entre DB y relés multifuncionales.	Las bases de datos reciben la información proveniente del EMS y se comunican continuamente con los relés multifuncionales.
4	Usar datos de predicción para conectar o desconectar una fuente de generación distribuida.	Consulta de disponibilidad de DER.	El dispositivo encargado de consultar la DB solicita información que le permita enviar datos de conexión o desconexión de alguna de las fuentes de generación distribuidas.
5	DER (s) conectada (s)/desconectada(s).	Nueva topología de la red.	El bloque selector analiza la nueva topología de la red debido a que se inicia operación en dos posibles casos: modo isla o conectado a la red. Adicionalmente puede deberse a la conexión o desconexión de DER en cualquiera de los dos casos.

Tabla 4.8. Pasos-escenarios: cambio de topología de la red

Escenario			
Nombre del escenario		**Cambio de topología de la red**	
No.	**Evento**	**Nombre del proceso/actividad**	**Descripción de proceso/actividad**
6	Cambiar condición operativa.	Análisis de selectividad para la nueva condición operativa.	El análisis realizado por el bloque selector hace un control de selectividad verificando si es necesario cambiar la configuración actual del sistema para la nueva condición operativa.
7	Usar factores de adaptación para cada dirección de flujo y cambiar características.	Estimación de corrientes de cortocircuito para cada dirección de flujo.	El relé multifuncional recibe continuamente las señales provenientes de DB, EMS y del bloque selector para estimar las corrientes de cortocircuito para cada dirección de flujo y cambiar las características de protección del sistema donde sea necesario.
8	Verificar si las nuevas condiciones operativas adaptadas por el relé sobrepasan las condiciones límites del sistema.	Comparación con condiciones límite.	Cuando las características de protección han sido actualizadas, el relé multifuncional compara los valores adaptados con las condiciones límite del sistema y se permitirá la nueva configuración si esas condiciones no son violadas. Si las condiciones límite son rebasadas no se permite la nueva configuración.
9	Permitir/no permitir cambio de topología	Decisión del sistema para aceptar o denegar el cambio de topología.	Si el cambio de topología es permitido se le enviará la información al relé multifuncional del cambio de topología y el esquema de protección comenzará a monitorear la nueva configuración de red. En caso de que sea denegado el cambio se le enviará una señal al EMS que le prohíbe la operación prevista.

Tabla 4.9. Pasos-escenarios: cambio de topología de la red (continuación)

Escenario			
Nombre del escenario		**Falla**	
No.	**Evento**	**Nombre del proceso/actividad**	**Descripción de proceso/actividad**
1	Recibir actualización del estado de la topología de la red.	Adquisición del estado actual de la red	El relé multifuncional recibe información del cambio de topología de la red y ajusta las configuraciones necesarias para actuar ante los eventos de falla que se presenten.
2	Monitorear continuamente ante posibles perturbaciones.	Detección continua de posibles fallas.	Continuamente se realizan mediciones y monitoreos en tiempo real a la red por medio de la información que llega al relé por parte de los equipos de medición y los sensores.
3	Comparar datos obtenidos a partir de mediciones e información suministrada por medidores y sensores.	Comparación de datos para determinar condiciones de disparo.	Al recibir constantemente las mediciones de la red, el relé multifuncional compara los datos recibidos y verifica si se cumplen o no las condiciones de disparo establecidas por la topología de red. El esquema de protección configurado estará siempre en alerta de posible disparo.
4	Se cumple la condición de disparo.	Detección de condición de disparo.	El relé multifuncional al realizar el análisis completo para verificar si los datos que está recibiendo y comparando, detecta que una o varias partes del sistema están en falla.
5	Apertura de interruptores en la(s) zona(s) afectada(s).	Decisión de disparo.	Una vez alcanzadas las condiciones de disparo el relé envía la orden de disparo a los interruptores que se encuentran en la zona de la falla para aislar la falla.

Tabla 4.10. Pasos-escenarios: falla

La segunda parte de las tablas, muestran el tipo de señal que producen los actores para ambos escenarios y son de utilidad para identificar los elementos que están haciendo el

intercambio de información en cada evento. Por su parte, los requisitos que hacen parte de la última columna de la tabla son extraídos de acuerdo con lo desarrollado en la sección 4.2.6.

Escenario					
Nombre del escenario		**Cambio de topología de la red**			
No.	**Servicio**	**Productor de la información (actor)**	**Receptor de la información (actor)**	**Información intercambiada (ID)**	**Requisitos (ID)**
1	CAMBIO	Bloque selector de configuración de protecciones	Relé multifuncional	I-07	Ti-Op-02 Ti-Op-03
2	INFORME	Transformadores de corriente y de potencial	Relé multifuncional	I-01	Pr-Da-01 Pr-Da-02 Ti-Op-02
3	EJECUTAR	Relé multifuncional	Relé multifuncional	I-05	Ti-Op-03
4	CREAR	Relé multifuncional	Relé multifuncional	I-08	Ti-Op-03
5	EJECUTAR	Relé multifuncional	Interruptor	I-08	Ti-Op-03

Tabla 4.11. Pasos-escenarios: falla (segunda parte)

Las tablas presentadas muestran el tipo de señal enviada, especificando el actor que produce la información y el actor que la recibe. Estas tablas tendrán la misma cantidad de pasos que se muestran en la primera parte.

Escenario					
Nombre del escenario		**Cambio de topología de la red**			
No.	**Servicio**	**Productor de la información (actor)**	**Receptor de la información (actor)**	**Información intercambiada (ID)**	**Requisitos (ID)**
1	INFORME	Medidor inteligente	Relé multifuncional	I-01	Pr-Da-01 Pr-Da-02 Ti-Op-02
2	CREAR	EMS	DB	I-02	Pr-Da-02
3	INFORME	DB	Relé multifuncional	I-01	Pr-Da-01 Pr-Da-02 Ti-Op-02
4	GET	Consulta en la DB	Bloque selector de configuración de protecciones	I-03	Ti-Op-03
5	EJECUTAR	Bloque selector de configuración de protecciones	Bloque selector de configuración de protecciones	I-03	Ti-Op-03
6	CAMBIO	Bloque selector de configuración de protecciones	Relé multifuncional	I-04	Ti-Op-02
7	CAMBIO	Relé multifuncional	Relé multifuncional	I-04	Ti-Op-02
8	EJECUTAR	Relé multifuncional	Relé multifuncional	I-05	Ti-Op-03
9	EJECUTAR	Relé multifuncional	EMS	I-06	Ti-Op-03

Tabla 4.12. Pasos-escenarios: cambio de topología de la red (segunda parte)

4.2.5 Paso 5: Identificar la información que se intercambia

Al tener claros los actores que interactúan en cada evento del escenario, se caracteriza la información que intercambian en el paso siguiente. Dentro de la estrategia de protección se realizan acciones como monitoreo de la red, comparación y almacenamiento de datos, entre otras. Los requisitos para el intercambio de información tienen que ver con la protección de datos y los tiempos de operación para evitar que se presenten fallas durante los cambios de topología. La información intercambiada es válida para ambos escenarios.

Información intercambiada			
Inf. ID	**Nombre de la información intercambiada**	**Descripción de la información intercambiada**	**Req. ID**
I-01	Monitoreo de la red.	El sistema de medidores inteligentes, sensores y base de datos envían informes del estado actual de la red.	Pr-Da-01 Pr-Da-02 Ti-Op-02
I-02	Almacenamiento de información en DB.	El sistema de gestión de energía almacena información de predicción en la base de datos que serán utilizados para determinar la disponibilidad de uno o varios recursos de generación.	Pr-Da-02
I-03	Informe de estado de disponibilidad de DER(s).	El bloque selector recibe información de disponibilidad y ejecuta acciones de conexión o desconexión de fuentes de generación.	Ti-Op-03
I-04	Nuevas condiciones operativas.	El relé recibe información de nueva topología y cambia sus configuraciones de protección estimando las corrientes de cortocircuito.	Ti-Op-02
I-05	Comparación de datos.	El relé multifuncional realiza comparación de datos obtenidos con valores y condiciones límite de la red.	Ti-Op-03
I-06	Señal de autorización o no autorización de cambio de topología.	Cuando el relé realiza la comparación define inmediatamente si la nueva topología cumple o no con las condiciones límite de la red.	Ti-Op-03
I-07	Información actualizada de topología de red.	El bloque selector confirma la configuración de la nueva topología al relé multifuncional.	Ti-Op-02 Ti-Op-03
I-8	Generación y envío de señal de disparo.	El relé puede generar un elemento de información que es enviado a los interruptores para aislar fallas.	Ti-Op-03

Tabla 4.13. Información intercambiada

4.2.6 Paso 6: Definir los requisitos necesarios para hacer efectiva la comunicación

Los requisitos se definieron siguiendo las descripciones de la estrategia de protección. Por ejemplo, se menciona que los tiempos de operación cuando se está haciendo un cambio de topología debe ser el mínimo posible para disminuir la posibilidad de que una falla ocurra mientras se conectan o desconectan fuentes de la microrred. Esa restricción da origen a una categoría llamada tiempos de operación (Ti-Op), que agrupa otros requisitos que tienen que ver con tiempos de operación del sistema. Por otro lado, hay otra categoría denominada protección de datos (Pr-Da) que tiene que ver con la comunicación y la seguridad de los datos que se almacenan para evitar el acceso de terceros. Estos requisitos serán mostrados en las tablas 4.14 y 4.15 respectivamente.

Requisitos		
Categorías ID	**Nombre de categoría para requisitos**	**Descripción de categoría**
Ti-Op	Tiempos de operación.	Esta categoría define los tiempos mínimos de operación de algunos elementos para evitar contingencias mientras alguna operación se esté realizando
Requisito ID	**Nombre de requisito**	**Descripción de requisito**
Ti-Op-01	Intervalos de monitoreo.	Las medidas realizadas por los medidores y sensores deben ser tomadas cada cierto tiempo establecido previamente.
Ti-Op-02	Tiempo de cambio de topología.	Los tiempos de cambio de topología deben tardar pocos segundos para disminuir las probabilidades de falla mientras se realice el cambio.
Ti-Op-03	Tiempo de generación de datos.	El análisis de datos y la generación de señales de disparo deben tardar el menor tiempo posible.

Tabla 4.14. Requisitos: tiempos de operación.

Requisitos		
Categorías ID	**Nombre de categoría para requisitos**	**Descripción de categoría**
Pr-Da	Protección de datos.	En esta categoría se tiene en cuenta los aspectos relevantes en cuanto al manejo y privacidad de los datos que se intercambian.
Requisito ID	**Nombre de requisito**	**Descripción de requisito**
Pr-Da-01	Comunicación remota.	Para la comunicación con elementos remotos (como interruptores) se requiere presencia de canales de comunicación confiables de alto ancho de banda.
Pr-Da-02	Almacenamiento de datos.	Los datos deben almacenarse de tal forma que se evite el acceso de agentes externos o de terceros que puedan alterar la información.

Tabla 4.15. Requisitos: protección de datos.

La tabla correspondiente a los términos y definiciones comunes de la sección 3.2.7 estará incluida en la sección A.1 de los anexos.

4.3 Etapa 3: Desarrollo de la estrategia de protección en una arquitectura de referencia

4.3.1 Paso 1: Desarrollo de la capa de componentes

A partir del diagrama de la figura 4.2 y las tablas desde la 4.2 hasta la 4.7, donde se identifican actores y escenarios de la estrategia de protección, se desarrolla la capa de componentes que se muestra en la figura 4.3. En esta capa se ilustran los actores y su ubicación se realiza de acuerdo con lo definido en el capítulo 2.

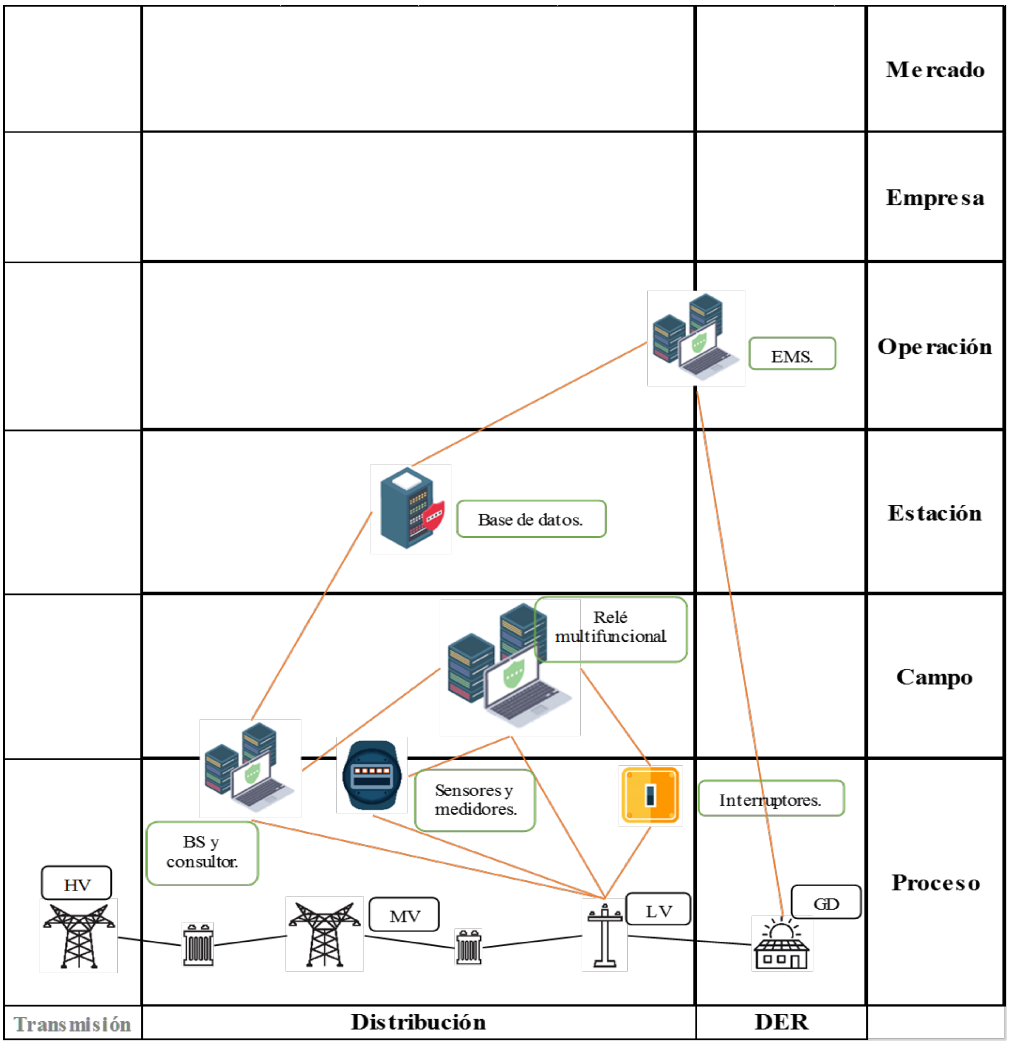

Figura 4.3. Capa de componentes

4.3.2 Paso 2: Desarrollo de la capa de negocios

Para la capa de negocios se utilizan los datos de la tabla 4.1 que menciona los casos de negocio relacionados y las restricciones posibles para implementar la estrategia de protección. Los casos de negocio que permite la estrategia son: mejoramiento de los índices de continuidad del suministro de energía, control de estabilidad, operación y protección de la microrred. Mientras que las regulaciones tendrán relación con las leyes nacionales o locales donde se vaya a implementar.

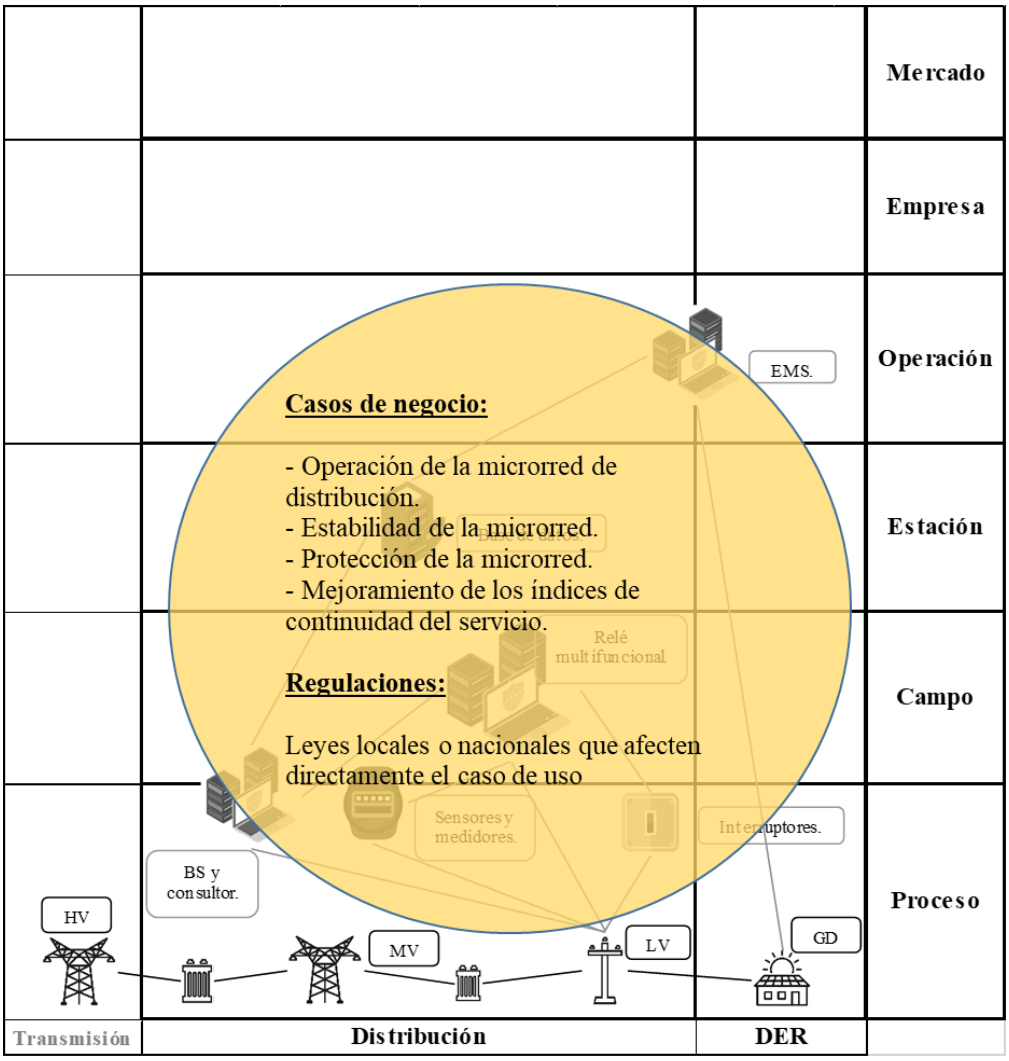

Figura 4.4. Capa de negocios

4.3.3 Paso 3: Desarrollo de la capa de función

Para el desarrollo de la capa de función se incluyen los escenarios de cambio de topología y de falla, en los dominios y zonas donde tengan mayor interacción de los actores. Las líneas rojas indican el intercambio de información de los actores que los afectan. Las tablas desde la 4.11 y 4.12 contienen la descripción necesaria sobre los actores que están intercambiando información para llevar a cabo los procesos de los escenarios de falla y cambio de topología, respectivamente. Esta capa se ilustrará en la figura 4.5.

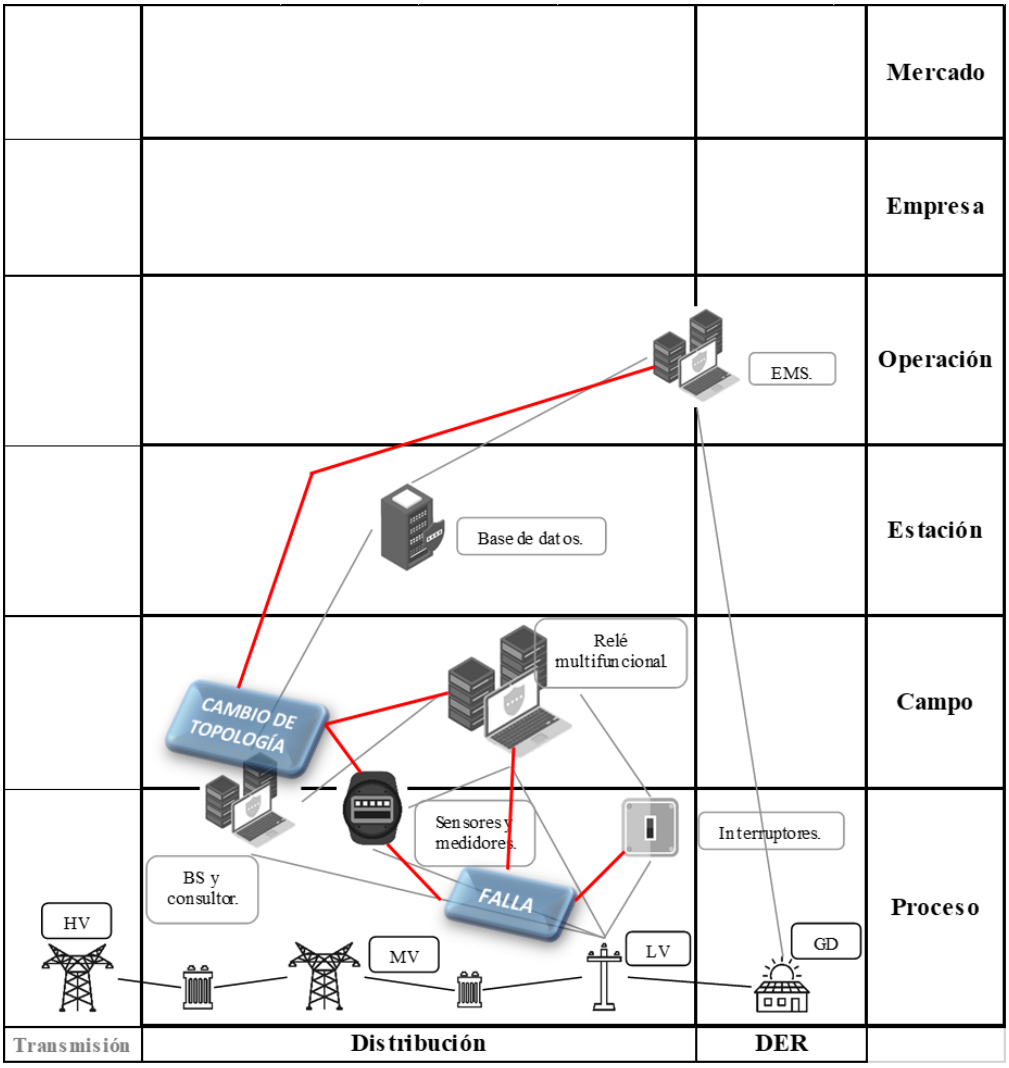

Figura 4.5. Capa de función

4.3.4 Paso 4: Desarrollo de la capa de información

La tabla 4.13 entrega la información que se intercambia, como se presenta en la figura 4.6.

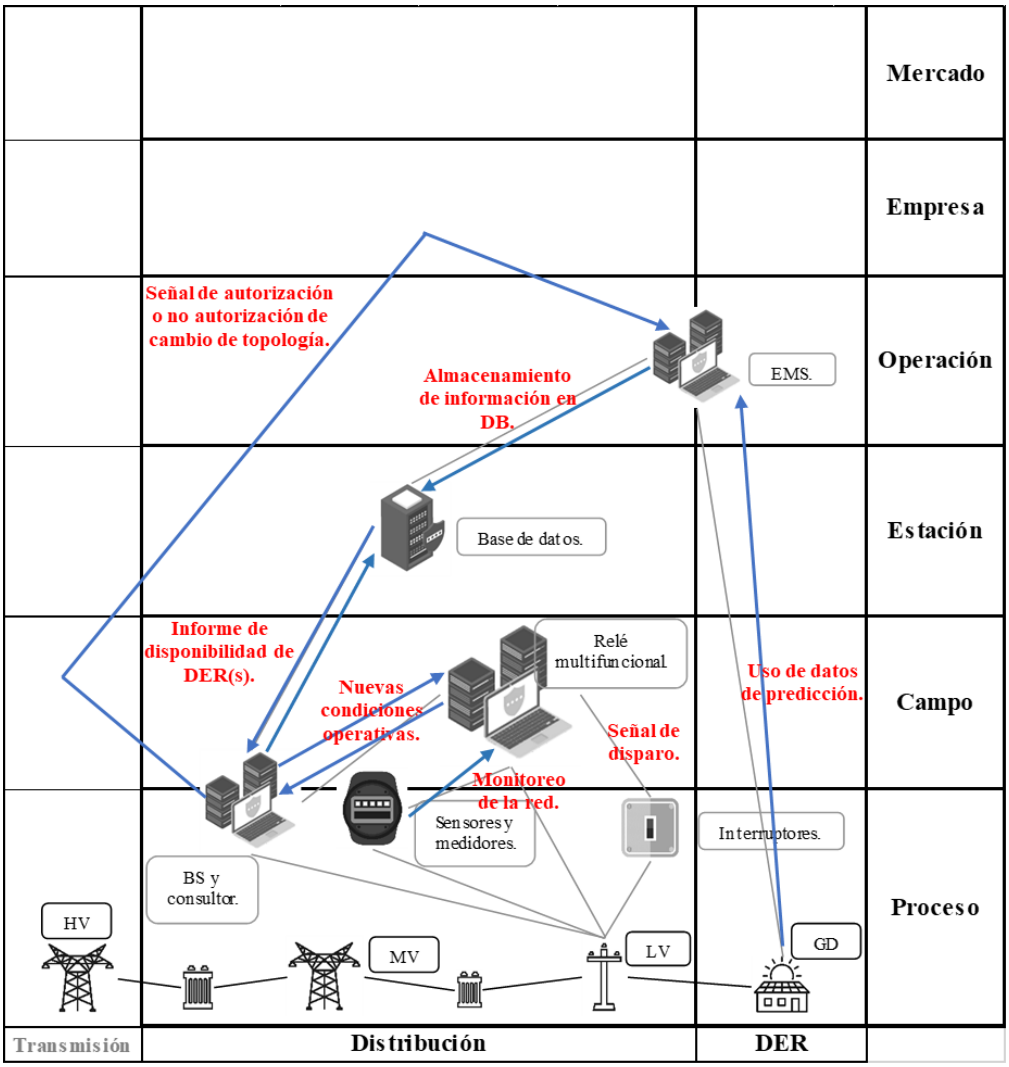

Figura 4.6. Capa de información

4.3.5 Paso 5: Desarrollo de la capa de comunicación

En la estrategia de protección descrita los protocolos de comunicación no son tratados en detalle puesto que no está dentro del alcance de este trabajo, sin embargo, se menciona el

estándar IEC 61850 necesario para la comunicación en tiempo real entre los elementos de medida y el relé multifuncional. Debido a esto, será el único protocolo descrito en la capa de comunicación que será mostrada en la figura 4.7.

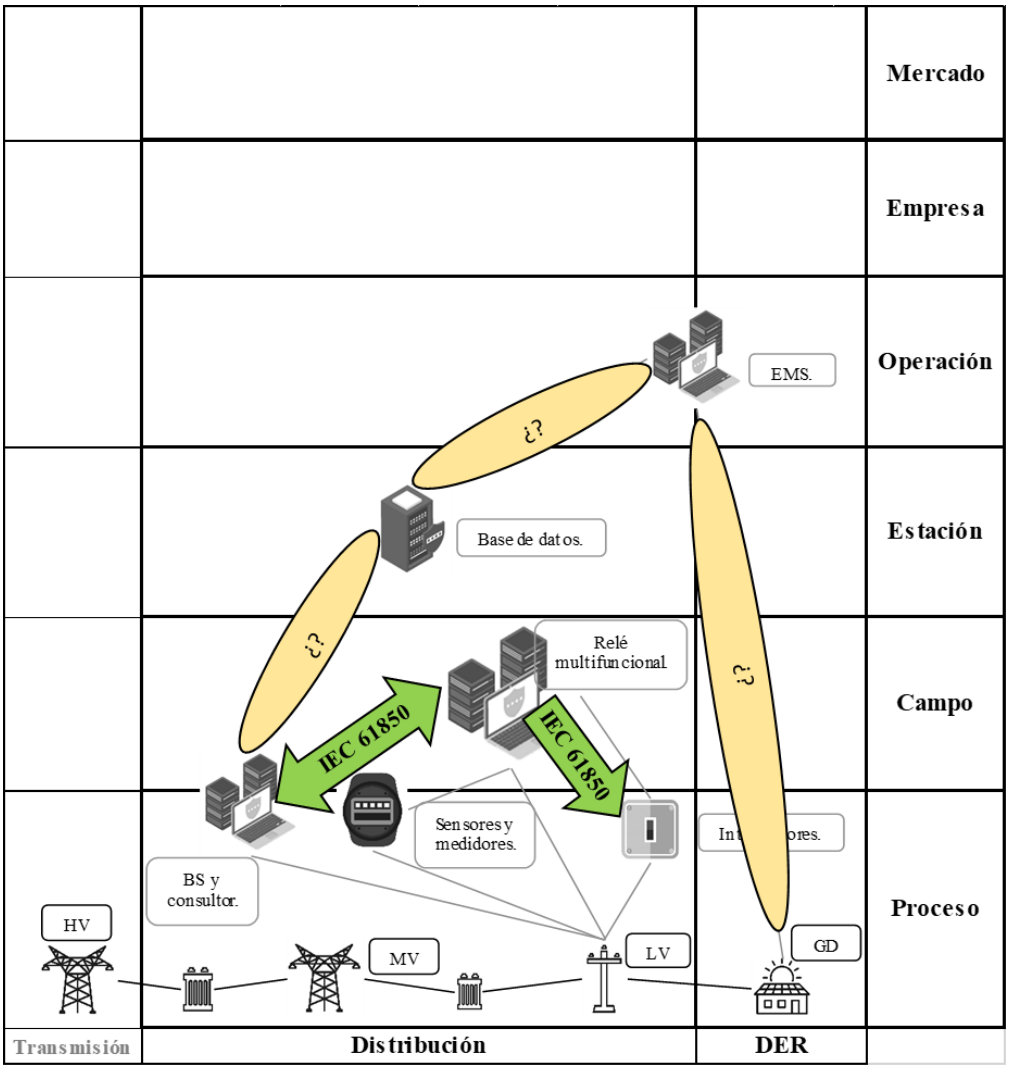

Figura 4.7. Capa de comunicación

Capítulo 5

Conclusiones y recomendaciones

5.1 Conclusiones

La investigación sobre estrategias de protección de microrredes basadas en comunicaciones permite identificar que los sistemas que hacen uso de medios de comunicación están basados en técnicas adaptivas, es decir, utilizan dispositivos de protección capaces de cambiar sus ajustes e intercambiar información entre ellos para proteger la red ante fallas. El uso de este tipo de esquemas presenta ventajas en cuanto a la rapidez para actuar ante contingencias, pero tiene desventajas en cuanto a la inversión, comparada con la de un sistema de protección convencional.

Las estrategias adaptivas basadas en comunicación pueden tener mandos centralizados o descentralizados, siendo más común el primero debido a que existen más protocolos de comunicaciones que lo soportan en comparación a un mando descentralizado. Sin embargo, los sistemas descentralizados presentan ventajas en cuanto a fallas que se puedan presentar en uno o varios de sus dispositivos. En caso que ocurra una contingencia de este tipo, el sistema descentralizado no se afecta en la toma de decisiones, mientras que, en el mando centralizado, un problema en el elemento principal producirá falla completa en el esquema de protección.

En cuanto a la inversión para cada mando es relativo, por ejemplo, para el control centralizado existe un alto costo de inversión en el elemento principal pero los demás elementos pueden ser más sencillos. Por su parte los esquemas descentralizados necesitan dispositivos capaces de intercambiar y analizar la información, que se traducirá en una gran inversión para todo el esquema. Por lo tanto, el uso de una estrategia de protección de este tipo debe ser analizada desde el punto de vista de las ventajas operativas que ofrece y el

costo de inversión.

El uso del estándar IEC 62559-2, el cual define una metodología para describir un sistema y los elementos que lo componen, es útil para definir y analizar el funcionamiento de cualquier estrategia de protección de microrredes. Seguir la plantilla que propone el estándar permite reconocer dispositivos, eventos y escenarios que son de utilidad para desarrollar la arquitectura de referencia, la cual requiere la especificación de estos elementos. Al ser identificados, es posible definir la información que intercambian y algunos requisitos que dependen del funcionamiento del esquema de protección para su implementación.

Describir una estrategia de protección de microrredes requiere representar de forma precisa los actores que intervienen debido a que deben ubicarse en lugares específicos en los dominios y zonas del marco SGAM. Este marco que incluye los elementos de la cadena de generación agregando el dominio de la generación distribuida, permite estandarizar los procesos que allí se describen, haciendo interoperable un proceso y, por lo tanto, más controlable por los operadores. Al añadir el dominio de las fuentes de generación distribuida, la metodología SGAM amplía su uso para redes inteligentes y procesos que incluyan este tipo de generación en su funcionamiento.

A pesar de que el esquema de protección descrito se desarrolla en dos dominios del marco SGAM: distribución y DER; es posible establecer comunicación con un proceso diferente que se encuentre en los mismos o diferentes dominios. El objetivo de la interoperabilidad, especificado en el estándar estudiado, es establecer comunicación a niveles tanto operativos como administrativos, por lo tanto, si se requiere comunicar un sistema con otro, es posible siempre y cuando se sigan protocolos adecuados para establecer el intercambio de información.

También es evidente la flexibilidad de la arquitectura de referencia en cuanto las nuevas funciones que se pueden agregar dentro del marco. Es decir, de igual forma como se incluyó un nuevo dominio para permitir su funcionamiento sin afectar su descripción, es posible adicionar nuevos elementos. La literatura consultada demuestra que el marco SGAM ha evolucionado para aumentar los dominios que lo componen como: vehículos eléctricos, arquitectura marina o la industria.

Finalmente, conocer e iniciar la investigación sobre estas herramientas y sus utilidades abren un panorama sobre las restricciones y estándares a tener en cuenta para implementar sistemas que emplean nuevas tecnologías. La arquitectura de referencia por medio de los pasos descritos en este trabajo pretende encontrar brechas o factores que impidan desarrollar completamente un sistema dentro de su arquitectura. No será suficiente plantear un esquema

de protección o cualquier otro esquema en alguno de los dominios, sin tener en cuenta las limitaciones, requisitos, protocolos o leyes nacionales que impidan su implementación.

5.2 Recomendaciones

Como se evidenció en el desarrollo de la arquitectura mostrada en el capítulo 4, los protocolos de comunicación no hicieron parte del enfoque de este trabajo y, como consecuencia de ello, no fue posible realizar la descripción total de la capa de comunicación mostrada en la sección 4.3.5. Por lo tanto, se recomienda como trabajo futuro que las investigaciones realizadas sobre sistemas que involucren intercambio de información se extiendan hasta los estándares que definen los protocolos necesarios para hacer efectiva la comunicación.

Adicionalmente en la bibliografía donde se estudian las aplicaciones de la arquitectura de red se manifiesta la posibilidad de expandir los dominios del marco SGAM. Estas expansiones se relacionan con las descripciones de funcionalidades de una ciudad inteligente, la inclusión de vehículos eléctricos, industria y arquitectura marina. Dichas expansiones pueden ser incluidas como nuevos dominios dentro del marco, demostrando la flexibilidad de la arquitectura. Por lo tanto, la profundización en estos nuevos campos pueden ser de interés para futuras investigaciones.

Anexos

Algunas de las partes del desarrollo de la arquitectura propuesta, que no se presentan en el capítulo 4, debido a que no influyen para comprender lo realizado, se muestran en este documento de anexos. Estas partes son importantes para la descripción de la estrategia de protección, y se presentan en orden de ejecución en estos anexos.

A.1. Describir de forma general el caso de uso.

Esta parte de la metodología, desarrollada en la sección 4.2.1, presenta el nombre del caso de uso, administración de versiones, narrativa del caso de uso, indicadores de rendimiento, condiciones del caso de uso y la información adicional sobre el caso de uso.

A.1.1. Nombre del caso de uso.

Para identificar el caso de uso se le da el nombre "estrategia de protección de microrredes basada en sistemas de comunicación", con un ID que agrupa las iniciales de las palabras que componen su nombre, presentada en la Tabla A.1.1.

Identificación del caso de uso		
ID	**Área: Dominio(s)/Zona(s)**	**Nombre del caso de uso**
Caso de uso de aplicación.	Dominios del marco SGAM/Zonas del marco SGAM	Estrategia de protección de microrredes basado en sistemas de comunicación.

Tabla A. 2.1. Identificación del caso de uso

A.1.2. Administración de versiones.

Los cambios realizados mientras la descripción fue realizada están presentados en la tabla A.1.2.

Gestión de versiones				
Versión no.	**Fecha**	**Nombre de los autores**	**Cambios**	**Estado de aprobación.**
1	02 de junio de 2019	J-D Orozco Álvarez	Creación inicial (Descripción general)	Borrador
2	17 de junio de 2019	J-D Orozco Álvarez A-R Herrera Orozco	Revisión general y definición de casos de negocio relacionados al caso de uso	Borrador
3	21 de junio de 2019	J-D Orozco Álvarez A-R Herrera Orozco	Definición de los indicadores clave de rendimiento	Borrador
4	22 de junio de 2019	J-D Orozco Álvarez A-R Herrera Orozco J-J Mora Flórez	Definición de actores y escenarios del caso de uso	Borrador
5	23 de junio de 2019	J-D Orozco Álvarez A-R Herrera Orozco J-J Mora Flórez	Revisión y corrección general del documento	Final

Tabla A. 2.2. Gestión de versiones

A.1.3. Narrativa del caso de uso.

La tabla A.1.3 muestra las descripciones breve y completa de la estrategia de protección basada en comunicaciones.

Narrativa del caso de uso
Descripción corta
Las estrategias de protección basadas en comunicación constan generalmente de un bloque (Análisis en tiempo real) de adquisición del estado actual de la red que además analiza posibles casos de contingencia que deben ser aislados y puede tomar decisiones de disparo de las protecciones. A este bloque en tiempo real se le establece comunicación con bloque en tiempo no real que se encarga de analizar las bases de datos generadas y administrar las fuentes de generación distribuida disponibles por medio de un mando central. Este bloque se encarga de consultar la disponibilidad de las fuentes y de verificar que las condiciones de disparo (condiciones límite) han sido sobrepasadas para enviar datos de disparo al bloque en tiempo real y realizar el accionamiento de las protecciones.
Descripción completa
Un esquema de protección inicia su procedimiento de análisis realizando una rutina de adaptación de las protecciones comunicando dos grandes bloques principales (Bloque en tiempo real y bloque en tiempo no real). Esto permite que exista un intercambio de información entre ambos bloques para mantener la red en funcionamiento y analizando las posibles configuraciones de la red al conectar y desconectar cualquiera de las fuentes distribuidas a lo largo del sistema de distribución. El bloque en tiempo real se encarga de adquirir los datos provenientes de la red verificando el estado actual y corroborando que se encuentre en condiciones operativas aceptables y, en caso contrario, activar las protecciones asistido por la información obtenida desde el bloque en tiempo no real verificando que los límites operativos del sistema sean suficientes o verdaderos para realizarlo. El bloque de tiempo no real recibe órdenes de conexión desde el bloque de tiempo real para realizar una conexión con las bases de datos que le provee un mando centralizado que administra las fuentes de generación distribuida disponibles del sistema. Después de solicitar y lograr la conexión a estas bases de datos se consulta la disponibilidad de las fuentes con la predicción que entregan las bases de datos y en caso de conectar o desconectar alguna de estas fuentes se solicita un control de selectividad. Este control de selectividad se encarga de ordenar las protecciones de manera que reconfiguren sus parámetros de disparo debido a que la red tiene una nueva configuración. En caso de que las protecciones al realizar los cambios de parámetros sobrepasen las condiciones límite del sistema, se le informará al mando centralizado que los cambios que se desean realizar al conectar o desconectar una o más fuentes, no será permitido. De otro modo, si las modificaciones que se desean realizar no sobrepasan los límites o no es necesario modificar las condiciones de disparo, se le consultará al bloque en tiempo real constantemente que realice un análisis con los datos actuales para que verifique si existen o no perturbaciones en el sistema que obliguen a cambiar el estado de las protecciones. El ciclo se repetirá indefinidamente.

Tabla A. 2.3. Narrativa del caso de uso

A.1.4. Indicadores clave de rendimiento.

Los indicadores identificados para implementar la estrategia de protección son: disminución de la duración y frecuencia de las interrupciones causadas por fallas, además de la operación y administración de la red facilitada por la comunicación entre los elementos.

Indicadores clave de rendimiento			
ID	**Nombre**	**Descripción**	**Referencia a los objetivos mencionados**
kpi_01	Duración y frecuencia de las interrupciones.	La instalación de un esquema de protecciones independiente de la estrategia utilizada se reflejará en una disminución considerable de los indicadores de continuidad del suministro asociados a duración y frecuencia de las fallas. A su vez permitirá disminuir la cantidad de usuarios aislados del suministro cuando ocurra evento no deseado en la microrred.	Mejorar la continuidad del servicio, mitigar el efecto de las fallas, incrementar eficiencia.
kpi_02	Monitoreo y administración de la red.	Implementar el esquema de protección con elementos capaces de recibir, analizar y enviar información permite que la red se pueda operar con mayor facilidad ante cualquier evento que se presente.	Obtener beneficios operacionales, maximizar el uso y capacidad de los activos de generación.

Tabla A. 2.4. Indicadores clave de rendimiento

A.1.5. Condiciones del caso de uso.

Las condiciones y sus respectivos prerrequisitos para que la estrategia de protección funcione correctamente, se presentan en la Tabla A.1.5.

Condiciones del caso de uso
Suposición
La implementación de este tipo de redes pueden verse afectadas por las regulaciones nacionales.
Prerrequisito
Las regulaciones nacionales sobre microrredes deben estar completamente definidas.
Suposición
Las protecciones utilizadas deben ser capaces de recibir, analizar y enviar información.
Prerrequisito
Tener disponibles relés digitales de protección multifuncionales e inteligentes con módulos de comunicación.
Suposición
Los elementos de medición envían oportunamente la información recolectada.
Prerrequisito
Los instrumentos de medición utilizados deben estar sincronizados entre ellos y operar de forma rápida.
Suposición
Los tiempos de toma de monitoreo, toma de decisiones y generación de información deben ser los mínimos posibles.
Prerrequisito
Los medidores, sensores y demás elementos que produzcan y envíen información deben ser de rápida operación.
Suposición
La red tiene condiciones límite y de disparo y corrientes de cortocircuito previamente establecidas.
Prerrequisito
Los relés utilizados deben ser adaptivos para fijar las condiciones del sistema.

Tabla A. 2.5. Condiciones del caso de uso

A.1.6. Información adicional sobre el caso de uso para clasificación

La relación que tiene la estrategia de protección seleccionada con otros casos de uso, el nivel de profundidad y las palabras clave para clasificarlo están mostrados en la Tabla A.1.6.

Información de clasificación
Relación con otros casos de uso
Esquema de protección de microrredes (incluido) / esquema de protección de microrredes basada en elementos adaptivos (asociado) / esquema de protección de microrredes basada en optimización (asociado) / Administración y control de variables eléctricas en la red de distribución (asociado)
Nivel de profundidad
Caso de uso genérico.
Priorización
Muy importante.
Relación genérica, regional o nacional
Genérica.
Naturaleza del caso de uso
Técnico.
Otras palabras clave para la clasificación
Protección de microrredes, administración de DER, protección basada en comunicación por mandos centralizados, protecciones adaptivas.

Tabla A. 2.6. Información de clasificación

A.1.7. Observaciones generales.

La Tabla A.1.7 muestra algunas observaciones identificadas y que no están especificadas en otra sección de la descripción del caso de uso.

Observaciones generales
• El procedimiento descrito a lo largo del caso de uso se desarrolla de manera descriptiva y general involucrando los actores que usualmente se encuentran en este tipo de estrategias. • La estrategia de protección basada en comunicaciones que se realiza en el caso de uso hace referencia a "Texto microrredes 1" citado en la sección 3.2 de este documento. • A pesar de ser describir una estrategia en particular, el procedimiento se hace de forma generalizada debido a que la mayoría de estrategias consultadas siguen un orden similar en la ejecución de sus actividades. • El caso de uso se desarrolla siguiendo la metodología IEC 62559.

Tabla A. 2.7. Información de clasificación

A.1.8. Especificar detalles técnicos.

En la sección 4.2.3 están definidos y agrupados los actores de la estrategia de protección. Los detalles técnicos requieren definir la bibliografía consultada y de utilidad para llevar a cabo la descripción.

Las referencias presentadas en las tablas siguientes tienen un impacto sobre el desarrollo de la descripción aportando conceptos útiles para lograrlo.

Referencias						
No.	**Tipo de referencia**	**Referencia**	**Estado**	**Impacto sobre el caso de uso**	**Origen/Organización**	**Link**
Electropedia	Sitio web	IEC electropedia		Medio	IEC	http://www.electropedia.org/
IEC 62559	Estándar	Use Cases - The IEC 62559 Methodology	Final	Alto	IEC	
Texto microrredes 1	Libro	Microgrids: Architectures and control	Final	Alto	Nikos Hatziargyriou/IEEE PRESS	
Texto microrredes 2	Libro	Microgrids and Active Distribution Networks	Final	Bajo	S. Chowdhury/S.P Chowdhury and P. Crossley	
Arquitectura de referencia	Estándar	Smart Grid Reference Architecture	Vol. 3.0	Alto	CEN-CENELEC-ETSI Smart Grid Coordination Group	
Paper 1	Publicación	Regional protection scheme for distribution network based on logical information	Vol. 11	Bajo	J. Ma/X. Xiang/R. Zhang/P. Li/J. Liu/J.S. Thorp	
Paper 2	Publicación	An integrated Wide-Area Protection Scheme for Active Distribution Networks Based on Fault Components Principle	Final	Bajo	F. Zang/L. Mu/W. Guo	

Tabla A. 2.8. Referencias

Referencias						
No.	**Tipo de referencia**	**Referencia**	**Estado**	**Impacto sobre el caso de uso**	**Origen/Organización**	**Link**
Paper 3	Publicación	A Communication-Assisted Protection Strategy for Inverter-Based Medium-Voltage Microgrids	Final	Bajo	M.A. Zamani/A. Yazdani/T.S. Sidhu	
Paper 4	Publicación	A Communication-Assisted Protection Strategy for Inverter-Based Medium-Voltage Microgrids	Final	Bajo	M.A. Zamani/A. Yazdani/T.S. Sidhu	
Paper 5	Publicación	A communication-based strategy for protection of microgrids with looped configuration	Final	Bajo	M.A. Zamani/A. Yazdani/T.S. Sidhu	
Paper 6	Publicación	Adaptive directional overcurrent relaying scheme for meshed distribution networks	Final	Bajo	D.S. Kumar/D. Srinivasan/A. Sharma/T. Reindl	
Paper 7	Publicación	Adaptive Protection and Microgrid Control Design for Hailuoto Island	Final	Bajo	H. Laaksonen/D. Ishchenko/A. Oudalov	

Tabla A. 2.9. Referencias (continuación)

Referencias						
No.	**Tipo de referencia**	**Referencia**	**Estado**	**Impacto sobre el caso de uso**	**Origen/Organización**	**Link**
Paper 8	Publicación	A Multiagent System-Based Protection and Control Scheme for Distribution System With Distributed-Generation Integration	Final	Bajo	Z. Liu/C. Su/H.K. Høidalen/Z. Chen	
Paper 9	Publicación	A Microgrid Protection System with Central Protection Unit and Extensive Communication	Final	Bajo	T.S. Ustum/C.Ozansoy/A. Zayegh	
Paper 10	Publicación	Principle and Implementation of Current Differential Protection in Distribution Networks With High Penetration of DGs	Final	Bajo	H. Gao/J. Li/B. Xu	
Paper 11	Publicación	Multiterminal Hybrid Protection of Microgrids Over Wireless Communications Network	Final	Bajo	T.S. Ustum/R.H. Khan	

Tabla A. 2.10. Referencias (continuación)

A.1.9. Definir términos y definiciones comunes.

Los términos y definiciones comunes utilizados para facilitar la comprensión del trabajo realizado se mostrarán en la tabla A.1.11 a continuación.

Términos y definiciones comunes	
Término	**Definición**
DB	Base de datos: Recopilación de datos organizados según una estructura conceptual (Véase IEC Electropedia: database).
DER	Son generadores (con sus equipos auxiliares, de protección y de conexión), incluidas las cargas que tengan un modo de generación (como los sistemas de almacenamiento de energía eléctrica), conectados a una red de baja o media tensión (Véase IEC Electropedia: DER).
EMS	Sistema de gestión de energía: Sistema de funcionamiento y control de los recursos energéticos y de las cargas de la microrred (Véase IEC Electropedia: Energy management system).
Falla	Estado del sistema en el que uno o más componentes no pueden funcionar como se requiere. Ejemplo: Cortocircuito, conductor roto y conexión intermitente (Véase IEC Electropedia: fault).
Microrred	Grupo de cargas interconectadas y recursos energéticos distribuidos con límites eléctricos definidos que forman un sistema local de energía eléctrica a nivel de tensión de distribución, que actúa como una única entidad controlable y es capaz de funcionar tanto en modo conectado a la red como en modo isla (Véase IEC electropedia: microgrid).
Relé	Dispositivo diseñado para producir cambios repentinos predeterminados en uno o más circuitos de salida eléctricos, cuando se cumplan determinadas condiciones en los circuitos de entrada eléctrica que controlan el dispositivo (Véase en IEC Electropedia: Relay).
Sistema de protección	Disposición de uno o más equipos de protección y otros dispositivos destinados a desempeñar una o más funciones de protección especificadas (Véase IEC Electropedia: protection system).
Transformador de corriente	Un transformador de corriente destinado a transmitir una señal de información a los instrumentos de medida (Véase IEC Electropedia: measuring current transformer).
Transformador de potencial	Un transformador de tensión destinado a transmitir una señal de información a los instrumentos de medida. (Véase IEC Electropedia: measuring voltage transformer).

Tabla A. 2.11. Términos y definiciones comunes

Bibliografía

Baghaee, H. R., Mirsalim, M., Gharehpetian, G. B. & Talebi, H. A. (2018), 'MOPSO/FDMT-based Pareto-optimal solution for coordination of overcurrent relays in interconnected networks and multi-DER microgrids', *IET Generation, Transmission & Distribution* **12**(12), 2871–2886.
URL: *http://digital-library.theiet.org/content/journals/10.1049/iet-gtd.2018.0079*

Behnke, R. P., Quero, D. O. & Mora, G. V. (2018), 'FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS'.

Briefs, S. & Energy, I. N. (n.d.), *Marion Gottschalk Mathias Uslar Christina Delfs*.

CEN, CENELEC & ETSI (2014), 'Report on Smart Grid Coordination Group: Smart Grid Information Security', (November), 1–107.
URL: *ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf*

Enanv, S. I. S., Medical, H., Ab, S. & Bertling, S. (2010), 'International Standard', **2004**.

Energía Eléctrica - Ministerio de Minas y Energía (n.d.).
URL: *https://www.minminas.gov.co/energias-renovables-no-convencionales*

Gottschalk, M., Uslar, M. & Delfs, C. (2017), 'The Use Case and Smart Grid Architecture Model Approach'.
URL: *http://link.springer.com/10.1007/978-3-319-49229-2*

Hatziargyriou, N. (2014), *Microgrid: Architecture and Control*, Vol. 1.

IEC 60050 - International Electrotechnical Vocabulary - Welcome (n.d.).
URL: *http://www.electropedia.org/*

Laaksonen, H., Ishchenko, D. & Oudalov, A. (2014), 'Adaptive protection and microgrid control design for Hailuoto Island', *IEEE Transactions on Smart Grid* **5**(3), 1486–1493.

Liu, Z., Su, C., Hoidalen, H. K. & Chen, Z. (2017), 'A Multiagent System-Based Protection and Control Scheme for Distribution System with Distributed-Generation Integration', *IEEE Transactions on Power Delivery* **32**(1), 536–545.

Ma, J., Xiang, X., Zhang, R., Li, P., Liu, J. & Thorp, J. S. (2017), 'Regional protection scheme for distribution network based on logical information', *IET Generation, Transmission & Distribution* **11**(17), 4314–4323.
URL: *http://digital-library.theiet.org/content/journals/10.1049/iet-gtd.2017.0560*

Microgrids, I.-b. M.-v. & Sidhu, T. S. (2012), 'A Communication-Assisted Protection Strategy for', *IEEE Transactions on Smart ...* **3**(4), 2088–2099.
URL: *http://ieeexplore.ieee.org/abstract/document/6295696/*

Ministerio de Minas y Energía (2018), 'Resolución No. 030 de 2018'.
URL: *http://apolo.creg.gov.co/Publicac.nsf/1c09d18d2d5ffb5b05256eee00709c02/83b41035c2c4474f05*

Muda, H. & Jena, P. (2017), 'Superimposed Adaptive Sequence Current Based Microgrid Protection: A New Technique', *IEEE Transactions on Power Delivery* **32**(2), 757–767.
URL: *http://ieeexplore.ieee.org/document/7555387/*

Piesciorovsky, E. C. & Schulz, N. N. (2017), 'Fuse relay adaptive overcurrent protection scheme for microgrid with distributed generators', *IET Generation, Transmission & Distribution* **11**(2), 540–549.
URL: *http://digital-library.theiet.org/content/journals/10.1049/iet-gtd.2016.1144*

Quintanilla, R. & Yarza, J. M. (2010), 'Nuevas exigencias y aplicaciones de comunicaciones para la protección de microrredes', *VI Seminario Internacional: SMART GRID en Sistemas de Distribución y Transmisión de Energía Eléctrica* pp. 43–50.
URL: *http://sg.cier.org.uy/publicaciones/revista.nsf/0a293b20eacdf8a903257133003ea67d/38d5383c4*

Rojas Pérez, G. T. (2018), '3.5% creció la demanda de energía en enero de 2018 en Colombia — El Mundo'.
URL: *http://www.elmundo.com/noticia/3-5crecio-la-demanda-de-energia-en-enero-de-2018-en-Colom*

Saavedra, M. A. (2017), 'Generación eléctrica en Colombia está holgada ante la demanda — El Mundo'.
URL: *http://www.elmundo.com/noticia/Generacion-electrica-en-Colombia-esta-holgada-ante-la-dema*

Saleh, K. A., Zeineldin, H. H., Al-Hinai, A. & El-Saadany, E. F. (2015), 'Optimal Coordination of Directional Overcurrent Relays Using a New Time–Current–Voltage Characteristic', *IEEE Transactions on Power Delivery* **30**(2), 537–544.
URL: *http://ieeexplore.ieee.org/document/6876231/*

Shiles, J., Wong, E., Rao, S., Sanden, C., Zamani, M. A., Davari, M. & Katiraei, F. (2018), 'Microgrid protection: An overview of protection strategies in North American microgrid projects', *IEEE Power and Energy Society General Meeting* **2018-January**, 1–5.

Specification, D. T. (2013), 'Draft Technical Specification'.

Ustun, T. S. & Khan, R. H. (2015), 'Multiterminal Hybrid Protection of Microgrids over Wireless Communications Network', *IEEE Transactions on Smart Grid* **6**(5), 2493–2500.

Ustun, T. S., Ozansoy, C. & Zayegh, A. (2011), 'A microgrid protection system with central protection unit and extensive communication', *2011 10th International Conference on Environment and Electrical Engineering, EEEIC.EU 2011 - Conference Proceedings* pp. 1–4.

Zamani, M. A., Sidhu, T. S. & Yazdani, A. (2013), 'A communication-based strategy for protection of microgrids with looped configuration', *Electric Power Systems Research* **104**, 52–61.
URL: *http://dx.doi.org/10.1016/j.epsr.2013.06.006*

Zhang, F., Mu, L. & Guo, W. (2019), 'An Integrated Wide-Area Protection Scheme for Active Distribution Networks Based on Fault Components Principle', *IEEE Transactions on Smart Grid* **10**(1), 392–402.